1. Abstract

2. Introduction

U.S. government agencies are now directed to assess the vulnerability of their operations and facilities to climate change and to develop adaptation plans to increase their resilience. Specific guidance on methods to accomplish these directives are still evolving based on the many different available frameworks. Our project was designed to develop and implement a vulnerability assessment framework for evaluating the vulnerability to climate change at a range of facilities in a portfolio of assets. This paper synthesizes lessons and insights from a series of research case studies conducted by the investigators at facilities of the U.S. Departments of Energy and Defense. The article elaborates on three sets of methods required to project exposure to hazards, evaluate consequences, and manage effective communications. In addition, suggested elements of a roadmap to support agencies in preparing for climate change, including additional methods development and capacity building, will be provided.

The literature contains a variety of proposals for conducting vulnerability assessments. . . . [insert lit review]

White House steps Step 1: Explore climate threats Step 2: Assess vulnerability and risks Step 3: Investigate options Step 4: Prioritize actions Step 5: Take action

In the next section we discuss some issues that we ran into while implementing these methods. Next we discuss our vulnerability assessment process. Finally, we discuss some additional takeaways from our case study experiences.

3. Musings on existing methods

In attempting to implement existing vulnerability methods at installations and sites in the Department of Defense and Department of Energy (DOE) portfolios we ran into several issues.

The first issue is that vulnerability analyses can have a variety of goals, outcomes, and stakeholders and there exists a tension in preventing vulnerability analyses from becoming a resource extractive effort. By this we mean that installation managers and below often have the information necessary to determine vulnerability but this information is not often cataloged, documented, etc. Thus, it takes time and effort on their part to put the pen to paper, fill out a new spreadsheet, sit in on presentations from academics, or be interviewed. But the benefits of conducting a vulnerability assessment tend to be long-term and more directed towards processes of the central offices (i.e., headquarters, departments, etc.). For example, changes in the vulnerability of an installation might feed into future siting decision making processes, which is clearly outside the purview of the installation level manager. But it is less apparent what the benefits of conducting a vulnerability assessment are to the daily functioning of an installation in the near-term.

This is not to say that vulnerability analyses, even with their longer-term focus, cannot provide useful information to installation level managers. For example, we found that installations tended to not know their existing vulnerabilities. In line with existing literature people are not computers and tend to have bad memories (weighting more recent events more heavily). Thus, it is a value added to conduct a

historical assessment of vulnerabilities that they care about. It is important to consider these types of issues given the necessary participation of these individuals in the VA process, even in non-democratic organizational structures like the military.

We found that the participatory process is a good way to conduct these exercises ... [Move participatory discussion here]

The second issue is the definition of vulnerability or a means of systematically evaluating vulnerability in a viable process. A related issue is the need to divorce vulnerability assessments from the limitations of existing climate models. It seems existing vulnerability assessment frameworks tend to get hung up on limits of projecting changes in exposure. Our framework pushes forward the idea that vulnerability and exposure are independent processes and that we can push forward on one even if the other is more limited.

Installation and facilities managers care about the consequences of climate change on their ability to meet mission (i.e., do the things they need to do). Our vulnerability assessment framework recognizes that consequences are the result of impacts, which are the intersection of vulnerability and exposure. By this we mean that an installation usually has a small set of vulnerabilities and the region also has a small set of exposures. Of these two relatively small sets there are usually only a few intersections (i.e., having both a vulnerability to a particular climate event and the climate event itself present).

The third issue we identify is that sites are often vulnerable to a small set of exposures (mentioned in the previous issue), which are often not variables generated in documents like the National Climate Assessment. For example, Fort Bragg is highly dependent upon fire management practices to manage their training ranges. Any changes in the ability to conduct prescribed burning activities could lead to impacts on the ability to conduct exercises. Therefore, the installation would like to know about changes to fire danger indices; however, these variables are not widely available at the country level let alone for the state or region.

4. Calls for a regional approach

The fourth issue we identify is that generating climate information outside of the data generated in processes like the National Climate Assessment is expensive. Regional climate outlooks are one way of reducing the cost of these exercises by spreading the cost across a larger group of stakeholders.

5. A three tiered approach

The final issue that we identify is creating some efficiency in the vulnerability analysis process. We know that exposure and vulnerabilities are not homogenous across a portfolio of assets, sites or installations. Instead, particular sites and assets are more vulnerable than others. Given this reality, it is economically inefficient to allocate vulnerability analysis resources evenly across the entire portfolio. We determined that a tiered approach to the process could be one way to overcome this challenge. Our tiered approach first uses institutional datasets (i.e., property management systems, GIS data, etc.) to create an indicator (i.e., a ranked ordering of all assets, sites, etc.) that determines the sites where further assessment is needed. In additional analyses, more and more resources are used at the site to identify particular vulnerabilities, impacts, and adaptation alternatives.

At least three tiers exist in the level of detail and analysis considered by a vulnerability analysis. Tier 1 screens all assets in an effort to guide the identification of assets at risk such that more detailed analyses can be undertaken at these locations. It would be inefficient to assume that all installations or assets are equally at risk from climate change. Tier 2 is a site level vulnerability analysis that identifies potential consequences and adaptation options using a participatory process. While the Tier 1 assessment results in an ordered list of sites for further analysis the Tier 2 analysis results in a set of vulnerabilities for the set of installations considered. The Tier 2 analysis identifies whether vulnerabilities need to be addressed through additional monitoring, altered management, or structural changes. It begins to assess the adaptation options necessary to improve resilience but these options are not yet evaluated at a level necessary for investment decisions. Tier 3 looks across the set of vulnerabilities identified in Tier 2 and identifies the cost effective solutions.

The users of a Tier 1 assessment are likely to be headquarters or major commands. The results of a Tier 1 assessment are meant to guide budget processes within the vulnerability assessment framework. In that it provides input to setting priorities for vulnerability assessments at installations.

An example of how one might go about doing a Tier 1 assessment is through the construction of a vulnerability indicator. In the case of the Department of Energy, which maintains the Facility Management System (FIMS); a real property database for the DOE. In the case of the DOE we looked at the average asset conditions by site for each program office in the DOE. Using the average and variance we were able to construct an indicator that identified sites with poor average condition of assets or sites with a high variance in terms of the condition of assets. The importance of the participatory process is evident in the indicator construction, as the weighting used for each asset should be a function of the importance of the asset to the mission. Some organizations have worked to develop such metrics (i.e., mission importance index in the DOE, unique facility indicator (DOE), etc.). But how much we should weight these assets could be developed in concert with stakeholders with the results evaluated using sensitivity analysis of the weights.

A Tier 2 analysis is developed in concert with installation personnel but produces information primarily for head quarters and major commands. The Tier 2 assessment can be useful in establishing long-term installation led processes to improve installation resilience. These activities might include improved data collection, maintaining databases, etc. One challenge of this process is that it might be considered as resource extractive process from the installation. The information collected will have a cost (i.e., increased man hours, etc.) but little direct benefit for the installation. By this we mean that the information collected might be more useful in guiding longer temr processes, which by definition fall under the purview of headquarters processes, rather than the day-to-day functioning of the installation.

This tension is further exacerbated by the need to engage installation managers in the process. Participatory process (guided learning) involving owners of key systems and subject matter experts. Require capacity building ... Discussion of the participatory process role in vulnerability analyses. Information is spread, many people have a portion of hte picture but few if any have the entire picture. Te process leans heavily on the knowledge of both headquarters and site personnel. A participatory process can synthesize site-specific expertise and technical inputs

needed to build resilience. Climate risk is a long-term process so building institutional capacity can provide some permanence to the process.

Tier 3: adaptation design Is the modification of engineering and planning processes to incorporate climate information. The challenge being to increase mutual comprehension of climate information needs and limits uses of climate projections produced under deep uncertainty. Begins with an assessment of vulnerability [Insert our definition of vulnerability]

Impacts are the intersection of exposure and vulnerability. Not all impacts have mission significance. Even though it hasn't been treated as such in budget processes enhancing resilience is a positive incentive.

Use of scenarios in vulnerability assessments. The scenarios should provide a broad range of future climate conditions, acknowledging the deep uncertainty that exists in the forcing, natural variability, etc.

6. Five steps and repeat: Vulnerability assessments

In this section we distill the results of the series of case studies we conducted to a set of steps for implementing a vulnerability analysis for an asset or site.

6.1. **Step 1: Establish assessment team.** Goal is to define the who, what, when and how, as well as setting expectations for the process. The team composition should include managers and technical experts related to key systems. In the military for example, the civilian workforce is often the vessel for the corporate memory (given how much military personnel move). The support of the installation leadership is critical in determining the outcome of hte processes.

The internal engagement process requires careful consideration, especially for data collection. In our case studies we tried two engagement processes. In the first, we provided some background materials before our initial kickoff meeting, in which we brought all of the interested (and important) parties together. The meeting was structured around providing information on climate change, climate change projections, impacts, and vulnerability assessments. Our efforts were primarily focused on gathering buyin and identifying what data existed and who managed it.

The alternative process involved identifying key stakeholders well in advance of the kickoff meeting. Generating buy in and soliciting data from these individuals and coming to the initial kickoff meeting with preliminary results. The goal of this process was to have a more informed discussion of where to go next (i.e., what do installation level managers need from us?). However, perhaps unique to the circumstances, we identified one significant weakness with this approach; it is highly dependent upon the quality of the information. In the particular case of Fort Bragg current documents had not been updated to reflect current conditions, which identified erosion as a major issue. While did not proceed as far as we might have down the erosion path, we did 'waste' some resources on this avenue.

External engagement focuses on the external dependencies. Subject matter experts are to facilitate expert judgment and identify the SMEs for specific topics.

6.2. **Step 2: Gather information and set priorities.** Objective is to gather and synthesize existing information and identify what topics require further assessment. Consider the upcoming decisions related to long-lived assets or future plans, not only current infrastructure/activities. This is an iterative process that relies

upon conference calls, document review, interviews, analysis and the use of extant documents and reports (i.e., INRMP, Master plans, etc.).

There are some key challenges to this step. The identification of climate thresholds is difficult. Attribute cancellations and damages to climate events (information capture could be improved). Assess adaptive capacity (key elements are intangible).

6.3. **Step 3: Obtain climate information.** Goal is to understand the state of science for climate phenomena that will drive future impacts. Distinguish information for participatory process and data for modeling. Sources for this information include the National Climate Assessment, CLimate Resilience Toolkit. We tested a climate change outlook approach, which is a document that assesses impacts relevant variables for facilities in the region. It uses historical climatology to establish baselines before then assessing global climate model output for projections. The regional coverage improves the economies of scale, as the report can be used across several installations. We found that it was useful but resource intensive and to be really useful would require that personnel support, manage, and disseminate the report.

6.4. **Step 4: Estimate/model impacts.** Goal is to gather and synthesize information on how vulnerabilities and future conditions could interact. Many sources and methods exist (a toolbox approach). Extrapolations from past incidents. Interpretation of assessements and research studies. Statistical analysis of observations The project budget is really going to determine the methods available.

6.5. **Step 5: Consider consequences and adaptations.** Objective is to evaluate the relative vulnerability and prioritize adaptation needs. Various spreadsheet and ranking tools facilitate this step. Importance of expert judgment of site and asset managers in considering the consequences of potential impacts. The key questions are given potential impacts, how might missions be affected? What next steps should be taken? Scenario planning and other engagement methods can be useful if participants are receptive.

6.6. **Step 6: Apply, document, and learn (cycle back to Step 1).** Do it all again! This is a process that is always in motion. Methods are improving, knowledge is improving, threats are emerging, etc.

7. Conclusions

Vulnerability assessments by their very nature are (or should be) circular. By this we mean, stakeholders should continue to evaluate not only their vulnerabilities through the process but also the process itself. As advancements are made in methods, models, etc. these changes should be incorporated into the process such that they are then necessarily incorporated in long-term decision making and planning activities. We see existing methods as getting the stakeholder to the right neighborhood (or city?), whereas future methods, models, or other advancements will get him or her to the right house.

In complying with the requirement to conduct vulnerability assessments, include objectives of building capacity and improving resources for climate risk management. Indicators, surveys, and stress tests can be used to systematically prioritize vulnerability assessments. We need to consider factors such as mission criticality, condition, and location relative to exposure. Site level vulnerability assessments can

contribute to resilience. Identify adaptation needs and build capacity for climate risk management.

Adaptation (i.e., changes in practices, infrastructure, etc.) should include improved monitoring. Collecting better information on impacts at a site is valuable for future risk management. Technical capacity is abundant, but more effort is required to organize it, share experience, and provide an evolving guide to resources. Stakeholder engagement, climate information, impacts estimation and modeling, etc.