STRENGTHENING OUR RESILIENCE TO ENVIRONMENTAL CHANGE IS A NATIONAL SECURITY IMPERATIVE

By Cathy Pennington

The accelerating pace of environmental change has given rise to a challenging array of domestic and global scenarios with high potential to destabilize domestic security and geopolitical equilibrium, threatening U.S. interests at home and abroad.

Regardless of the causes of environmental change, creating resilience to meet these impending challenges is a national security imperative that will require a comprehensive national-level strategy, open data sharing in strong partnership with industry, and a common resilience framework that enables consistent prioritization of adaptation investments across regions and localities.

Mounting Recovery Costs

Recovery from the destruction brought by coastal flooding, extreme weather, wildfires, and droughts is already costing the United States billions of dollars per year, and is putting at risk the systems, infrastructure, and institutions that collectively comprise our national security. As climate-related disasters increase in frequency and severity, replacement costs are mounting.

In January 2019, the Department of Defense (DoD) stated in a report to Congress that the effects of a changing climate are a national security issue with potential impacts to the department's missions, operational plans, and installations. [Office of the Under Secretary of Defense for Acquisition and Sustainment, Report on Effects of a Changing Climate to the Department of Defense, January 2019] DoD manages a global real-estate portfolio with an almost $1.2 trillion estimated replacement value. With each new disaster, the loss of infrastructure, base access, and personnel productivity has been acknowledged as negatively affecting force readiness. Additional costs in military family health, loss of base support services, and surrounding community infrastructure support compound the losses, and are being borne domestically and at U.S. government and military installations worldwide.

- Naval Station Norfolk, which suffers from persistent, recurring flooding due to tidal changes, has begun to build double-decker piers costing more than $100 million each to counter ground subsidence and rising seas.
- Repairs from flood damage at Tyndall AFB and Offutt AFB will take years to complete and are estimated to collectively cost the Air Force almost $4 billion.
- The Marine Corps estimated $3.6 billion to repair the damage to more than 900 buildings caused by Hurricane Florence in 2018.

Impacts to National Security Go Far Beyond Recovery Costs

According to the Center for Climate and Security, "The world is very likely to experience more intense and frequent climate shocks that could swiftly destabilize areas already vulnerable to insecurity, conflict, and human displacement, as well as those regions whose stability is brittle due to underlying geographic and natural resource vulnerabilities. The resulting resource scarcity, population migration, and social and political disasters are likely to interact at the international level, alongside the creation of new areas of great power competition and potential conflict." [A Security Threat Assessment of Global Climate Change: How Likely Warming Scenarios Indicate a Catastrophic Security Future, Center for Climate and Security, February 2020]

Extreme weather in the United States has exposed the fragility in our national systems, infrastructure, and institutions. The health effects of extreme heat are of growing concern in the desert southwest as indications of an impending megadrought become increasingly apparent. Desertification and associated reductions in agriculture production and potable water may lead to food and water insecurity among the most vulnerable. Recurring wildfires in the West threaten infrastructure and human life. As incidences of drought, wildfire, flooding, and extreme heat increasingly occur, larger segments of our population will be impacted, with the potential for climate retreat from affected areas. Those most vulnerable to poverty or homelessness will often be most affected, further highlighting social inequities and potentially leading to domestic unrest.

Creating Resilience at Scale

Our national security depends on building greater resilience against the effects of environmental threats. In June 2019, the GAO issued a report that recommended enhanced planning for climate resilience to help limit the federal government's fiscal exposure. They stated, "Enhancing climate resilience means being able to plan and prepare for, absorb, recover from, and more successfully adapt to climate-related impacts" [Climate Resilience: DoD Needs to Assess Risk and Provide Guidance on Use of Climate Projections in Installation Master Plans and Facilities Designs, Report to Congressional Requesters, June 2019, GAO-19-453] A comprehensive approach is needed — one that involves all levels of government in setting and monitoring goals; that employs open sharing of data and results

> Increasing Impacts of Environmental Change Demand New Strategies to Create Resilience at Scale and Preserve Our National Security Advantage.

across national, state, and local portfolios of adaptation investments; and that promotes a seamless boundary with industry stakeholders to improve resilience in our critical national systems and infrastructure.

National Strategy. To build true resilience, a comprehensive national strategy is needed that provides a framework of goals, investments, and objective measures to guide public and private policy and investment strategies at the federal, state, and municipal levels. At the federal level, this strategy must involve all branches of government, addressing the broad nature of impacts across our national systems. Further, development of this strategy must involve both government and industry in setting goals for mitigation and adaptation and creating public-private partnerships for investment in resilient solutions.

Open Sharing of Data and Results. Resilience cannot be achieved by a patchwork of solutions optimized to meet local needs. As investments are made in adaptation, these need to be optimized beyond local levels, to ensure common concerns are prioritized with similar emphasis. Data regarding priorities, efficacy of solutions, and investment ROI must be shared to optimize and tune for best resilience at a cross-regional level.

Strong Partnership with Industry. Our nation's critical systems and infrastructure are operated as a broad partnership among government and industry. As we learned from the last decade of dealing with cyber threats, critical information regarding vulnerabilities, risks, and countermeasures must be openly shared in partnership with industry.

Common Resilience Framework: Applying Proven Threat/Vulnerability/Risk Modeling Techniques to Improve Resilience

In our current national security posture, the allocation of resources to environmental adaptation and resilience is in competition with many other urgent priorities. To support a national strategy, we recommend a common environmental security resilience framework to effectively enable the detailed analysis and prioritization necessary to make the best use of available resources for adaptation and resilience.

MITRE's experience in bringing communities together to develop more effective cybersecurity approaches provides a parallel experience from which we can draw important lessons. MITRE ATT&CK® is a globally accessible knowledge base of cyber tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community. The same partnership-based approach can be employed to develop improved climate threat modeling, vulnerability analysis, and risk assessments, as a community and shared as a common framework to create more robust approaches, thereby yielding deeper resilience.

Borrowing from MITRE's experience with the ATT&CK framework, we have applied those insights and approaches to develop an environmental security "Resilience Framework" to provide improved approaches for threat modeling, vulnerability analysis, and risk assessment — which comprise the foundation for prioritization and optimization of investments in adaptation and resilience.

Improved Threat Modeling. To increase the effectiveness of threat modeling, policymakers need to understand more deeply the ways in which environmental threats, such as those shown in Figure 1, behave as a cascading series of increasingly persistent and increasingly destructive effects over time. Predictive modeling of cascading effects at regional levels should be the foundation for resilience planning, and those predictions, which will drive significant investment and hard tradeoffs, will require coordination and agreement across multiple levels of government.

Sea Level Rise	Coastal Flooding	Coastal Erosion	Taxable Land Loss	Inland Salinity
Warmer Air Temperatures	Drought	Wildfires	Arable Land Loss & Agriculture Disruption	Inland Flooding
	Reduced Potable Water	Crop and Forest Pests	Heat Stress	Vector-borne Disease
Rising Ocean Temperatures & Acidity	Glacier Melt and Debris	Aquatic Ecosystem Destruction	Fisheries Decline / Migration	Water-borne Pathogen Emergence
Extreme Weather	Greater Extremes in Temperatures and Events	Increased Frequency in Extreme Events	Increased Turbulence	Unstable Seasonality

Figure 1. Environmental Threats

Deeper Vulnerability Analysis. During the current COVID-19 pandemic, the brittleness of national systems and institutions that we had previously thought invulnerable has been exposed. It is imperative to understand where and how we are vulnerable to emerging threats, whether from a pandemic, cybersecurity, or environmental change. Governments must partner with industry to perform vulnerability analyses of our key systems and institutions, such as those illustrated in Figure 2, to assess where and how they may be affected by environmental change, and the resulting impact on national security. This must be done across regions and localities, in partnership with industry, while considering national level equities. Protection of industry and company-sensitive information is paramount as well, so the results of vulnerability analyses, which must be shared for common effect, must also be appropriately protected and anonymized.

Critical Infrastructure	Human Health	Military Readiness	Public Safety	Economic Stability	Geopolitical Stability
Energy	Food/Water Security	Ports, Bases & Airfields	Law Enforcement	Agriculture & Fisheries	Resource Contention
Communica-tions	Healthcare Delivery	Safety of Navigation	Border Control	Natural Resources	Local Instability
Public Utilities	Medical Supply Chain	Military Systems	Judiciary	Housing	Famine & Thirst
Transporta-tion	Heat Illness	Military Supply Chain	Emergency Medical	Education	Mass Migration
Hospitals	Allergens & Respiratory	New Missions	Public Sanitation	Employment	Failed States
Dams & Bridges	Mental Health	Military Health	Fire and Rescue	Goods and Services	New Conflict Zones

Social Equities and Social Justice

Figure 2. Vulnerable National Security Systems

Understanding Risk and Projecting Impact Over Time. We encourage governments at the federal, state, and local level to participate in adoption of common risk-assessment methodologies to predict and prioritize impact in terms of loss (physical, economic, operational), damage, or destruction, and to execute these on an ongoing basis with continuous monitoring and adjustment over time.

Recommendations

Addressing climate change is a "whole of nation" responsibility. To create resilience at scale and preserve our national security, MITRE recommends the following actions to be led at the federal level:

Develop a Comprehensive National Strategy. A comprehensive national strategy is needed that provides a framework of goals, investments, and objective measures to guide public and private policy and investment strategies at the federal, state, and municipal levels. Development of this strategy must involve both government and industry in setting goals for mitigation and adaptation and creating public-private partnerships for investment in resilient solutions.

Promote Open Sharing of Data and Results. Resilience cannot be achieved by a patchwork of solutions optimized to meet local needs. As investments are made in adaptation, these need to be optimized beyond local levels, to ensure common concerns are prioritized with similar emphasis. Data regarding priorities, efficacy of solutions, and investment ROI must be shared to optimize and tune for best resilience at a cross-regional level.

Ensure Close Partnership with Industry. Our nation's critical systems and infrastructure are operated as a broad partnership among government and industry. As we learned from the last decade of dealing with cyber threats, critical information regarding threats, vulnerabilities, risks, and countermeasures must be shared in partnership with industry, while protecting industry equities.

Employ a Common Resilience Framework. To support a national strategy, we recommend a shared environmental security resilience framework to effectively enable the detailed analysis and prioritization that must occur to make the best use of available resources to invest in adaptation and resilience.

Consider the Formation of Environmental Information Sharing and Analysis Centers (ISACs). ISACs are trusted entities established by critical infrastructure owners and operators to foster information sharing and best practices about physical and cyber threats, vulnerabilities, and mitigation. The concept of ISACs was introduced and promulgated pursuant to Presidential Decision Directive-63 (PDD-63). The ISAC concept should be extended to enable sharing of environmental threat, vulnerability, and risk information between government and industry via the creation of new Environmental Security Analysis Centers (ESAC).

We believe the time to act and the opportunity to make a difference is now. While ideological and political debate will continue about the causes of environmental change, the fact that risks exist to our national security and infrastructure remains. It is incumbent on government, the private sector, researchers, and policymakers to come together to address the accelerating risk level and develop data-driven solutions. We believe this framework can serve as the context in which these partnerships can form, and data can be shared to collectively and collaboratively take actions in the interest of national security.

For more information about this paper or the Center for Data-Driven Policy, contact policy@mitre.org