# Resilience Assessment in Homeland Security

Frédéric Petit[i*]

**Keywords:** Critical infrastructure, infrastructure interdependencies, resilience assessment, homeland security

[*]Corresponding author: fpetit@anl.gov

## Definition of resilience

The need to understand and enhance the protection of the United States critical infrastructure has been a national focus since the President's Commission on Critical Infrastructure Protection was established in 1996 (President's Commission on Critical Infrastructure Protection, 1997). Although resilience has been defined and studied in several fields (e.g., ecology, social science, economy, and computing) since the 1970s, it is only recently that this concept is used in homeland security for the management of critical infrastructure systems.

In 2011 and 2013, the release of Presidential Policy Directive (PPD)-8 on National Preparedness and PPD-21 on Critical Infrastructure Security and Resilience expanded on the importance of understanding the resilience of citizens, communities, and critical infrastructure. PPD-8 aimed at strengthening the security and resilience of the United States by directing the development of a national preparedness goal that identifies the core capabilities necessary for preparedness and a national preparedness system to guide activities that will enable the resilience enhancement of the nation (DHS, 2011). PPD-21 is more specific to critical infrastructure because it establishes the roles and responsibilities of the Secretary of the Department of Homeland Security (DHS) to strengthen the security and resilience of all 16 critical infrastructure sectors. PPD-21 specifically calls for operational and strategic analysis to inform planning and operational decisions regarding critical infrastructure and to recommend resilience enhancement measures (The White House, 2013).

Following the work conducted by the National Infrastructure Advisory Council (NIAC, 2009) (NIAC, 2010) and the National Academies of Sciences, Engineering, and Medicine (The National Academies, 2012), PPD-21 defined critical infrastructure resilience as "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions." (The White House, 2013)

Resilience is therefore about the change of state of the infrastructure system and integrates the system's capability to adapt and transform its operations to deal with stresses and maintain an acceptable level of functioning. Assessing resilience requires to consider the evolution of the state of the infrastructure system over time, and to determine both the amount by which the activity/well-being declines and the amount of time required to return to the pre-event level of operations or to a new level of equilibrium. Therefore, elements characterizing the capabilities of the infrastructure systems both before (i.e., anticipation, resistance, and absorption) and after (i.e., response,

[i] Decision and Infrastructure Sciences Division, Argonne National Laboratory

Suggested citation: Petit, F. (2018). Resilience assessment in homeland security. In Trump, B. D., Florin, M.-V., & Linkov, I. (Eds.). *IRGC resource guide on resilience (vol. 2): Domains of resilience for complex interconnected systems.* Lausanne, CH: EPFL International Risk Governance Center. Available on irgc.epfl.ch and irgc.org.

adaptation, and recovery) an adverse event occurs are important to consider in resilience definition and strategies.

The 2013 edition of the National Infrastructure Protection Plan followed PPD-21 and reinforced the need to “enhance critical infrastructure resilience by minimizing the adverse consequences of incidents through advance planning and mitigation efforts, and employing effective responses to save lives and ensure the rapid recovery of essential services” (DHS, 2013).

These strategy documents are completed by government agencies’ strategic plans that operationalize the consideration of both security and resilience measures in risk management approaches. DHS has developed several of these plans. The DHS Office of Infrastructure Protection (IP) Strategic Plan 2012–2016 establishes the goals for the DHS IP to improve risk management activities and enhance resilience through better understanding of critical assets, systems, and networks’ operations (DHS, 2012).

In 2015, the DHS developed the National Critical Infrastructure Security and Resilience Research and Development Plan (CSIR) to guide prioritization of research and development efforts within DHS. Among the tenets articulated for the CISR, is that “[m]etrics, standard methods of assessment, and baselines must continue to be developed and refined to effectively measure resilience” (DHS, 2015).

DHS has also developed specific programs, such as the Regional Resiliency Assessment Program (RRAP), to address the objectives of its strategic plans. RRAP is an interagency and cooperative assessment of specific critical infrastructure within a designated geographic area (DHS, 2017). RRAP projects are initiated to respond to stakeholders’ requirements. Some RRAPs specifically analyze infrastructure systems and propose resilience enhancement options and operational alternatives to reinforce the robustness of critical infrastructure.

Critical Infrastructure are complex networks mandated to provide resources and services that support the functioning of a socio-economic society and to satisfy its basic needs. Thus, it is necessary to keep these systems operational both on a daily basis and in time of emergencies. Resilience strategies represent a shift in traditional risk and emergency management perspectives from attempting to control changes in systems that are assumed to be stable, to sustaining and enhancing the capacity of socio-technical systems to adapt to uncertainty and emerging threats.

Ultimately, the main goal of resilience strategies is to enable decision-makers to make informed choices that will result in cost-effective reductions in the level and duration of consequences associated with the range of potential natural and man-made threats. When risk management strategies focus more on enhancing the protection of critical infrastructure to probable hazards, resilience strategies seek more specifically to promote business continuity and continuity of operations to enhance infrastructure systems’ emergency management capabilities to cope with unanticipated threats (i.e., the famous black swan events).

In the last 20 years, U.S. policies addressing critical infrastructure evolved from privileging risk management approaches focusing on protection against man-made threats to all-hazard approaches considering both security and resilience management strategies.

Even if the concept of resilience is defined in national policies, discussions are still ongoing about the resilience components, the relationship between risk and resilience, and the characterization of resilience metrics. One of the main concerns is the absence of industry or government initiative to develop a consensus on or to implement standardized assessment approaches (DOE, 2017). To address this issue for the energy sector, the U.S. Department of Energy (DOE) developed the DOE Grid Modernization Laboratory Consortium (GMLC) with the objective to help shape the future of the electric grid and ensure its protection and resilience (DOE, 2018). Among all initiatives conducted by the GMLC, one project specifically addresses the development and application of analysis metrics (i.e., reliability, resilience, sustainability, flexibility, affordability, and security) for assessing the evolving state of the U.S. electricity system and monitoring progress in modernizing the electric grid (GMLC, 2017).

**Resilience: A component of risk management**

Over the ages, traditional approaches of critical infrastructure protection have focused mainly on the consideration of consequences and vulnerability to man-made hazards. However, methods used to define and analyze risk are constantly evolving. This evolution of homeland security from protection to the resilience of the Nation and its critical infrastructure raises a question about the relationship between risk and resilience.

Risk is traditionally defined as a function of three elements: the threats to which an asset is susceptible, the vulnerabilities of the asset to the threat, and the consequences potentially generated by the degradation of the asset. If risk is a function of threats and hazards, vulnerabilities, and consequences, the challenge is to define where and how resilience fits into the determination of risk? The answer to this question is difficult yet important because it supports the development of risk and resilience assessment methodologies.

As identified in national policies, such as the 2013 National Infrastructure Protection Plan, (DHS, 2013) risk management includes resilience, as well as promoting an all-hazards approach that integrates man-made threats and natural hazards. This evolution constitutes a major change of paradigm in terms of homeland security. Ways to assess risk to critical infrastructure have evolved, from methods that were based only on protective measures and vulnerability, to methods that integrate resilience.

In order to manage critical infrastructure effectively from a “risk perspective,” it is necessary to form an approach that is not based exclusively on protection and prevention. Risk and emergency management must include a balance between preparedness, mitigation, response, and recovery. The progression of risk management for critical infrastructure must consist of an evolution and incorporation of resilience and service continuity, a more comprehensive involvement of all stakeholders (including the public) based on strong information sharing, and training and education processes that includes the effects from infrastructure interdependencies.

Even if in recent homeland security policies and business standards, resilience concepts are included in risk management strategies, a distinction can be made between strategies seeking to eliminate or transfer the risk and strategies seeking to maintain critical infrastructure operations. The first type of strategies, usually named risk management strategies, tries to eliminate negative consequences by implementing protection measures that reduce threats and vulnerabilities. The second type of strategies tries to maintain consequences at an acceptable level by implementing preparedness, mitigation, response, and recovery measures. In general, protective measures are specific to a threat type and they obviously require knowing the threat.

Resilience measures, on the other hand, can be specific to a given threat or can be general to apply to not yet identified threats. When, for protective measures, failure is not an option, resilience measures require to envision failure as being possible and to implement capabilities that will allow the system to react, adapt, and potentially transform. Resilience strategies require flexibility that can be supported by strong collaboration and information sharing mechanisms, but also by the development of business continuity and emergency management planning and exercises.

Risk management and resilience management strategies are inseparable and complementary. Risk management strategies are implemented to mitigate known threats and resilience management strategies are implemented in case the protection measures are not sufficient to prevent negative consequences resulting from known or unknown threats. Comparing the costs of risk management or resilience management strategies is difficult. It depends on so many factors including the difficulty to define the return on investment and to prove that the absence or limitation of critical infrastructure dysfunctions result from the implementation of management strategies. Implementing resilience strategies requires changing traditional risk management approaches to consider both known and unknown hazards, and to base the assessments on critical infrastructure capabilities to cope with unidentified low probability high impact events. It is therefore difficult to justify investments and define resulting return on investments when the threats and their consequences are by definition unknown.

However, developing resilience management strategies to enhance the flexibility and adaptability of critical infrastructure systems is always beneficial to maintain the systems' operations at an acceptable level and this whatever the type and importance of threat or hazard.

**Resilience strategies to reduce undesired consequences**

Comprehensive risk and resilience management strategies require collaborative and multidisciplinary approaches to combine social, economic, and technical points of view to fully elucidate the full range of influences acting upon an organisation, from the individual asset to the system level. This requires combining social and system engineering methodologies to inform multi-organisational decision-making and prioritize activities to reduce consequences duration and importance, and therefore maintain acceptable levels of critical infrastructure operations.

The next generation of resilience management methodologies needs to be developed at a regional level. The tendency for critical infrastructure to be managed and regulated in isolation from one another hampers the understanding of challenges arising from interdependencies. Resilience management approaches need to move beyond developing business continuity and emergency management plans that focus mainly on facilities and assets, to developing plans that consider regional resilience management capabilities and integrate elements that may be outside of one organization's control. It is not sufficient to have generators, fuel storage, and refueling priority to prepare for a power outage. Enhancing the protection and resilience of critical infrastructure requires the promotion of regional coordination, the definition of restoration priority, and the reallocation of resources to limit consequences and channel potential cascading failures. Critical infrastructure should determine which of their missions, functions, and assets are critically dependent on the services or resources provided by other organizations.

After prioritizing their operations, critical infrastructure should organize collaborative and secure exchanges with their suppliers and regional emergency managers to coordinate decision-making and achieve the greatest benefit for the most critical needs. The definition of an acceptable level of consequences is the first potential drawback for implementing resilience but also risk management strategies. Conceptually (and before an event), it is relatively easy to decide to prioritize response and recovery activities, and to decide to channel the consequences resulting from cascading and escalating failures. The reality may be different when the adverse event occurs. The main challenge is to define the risk ownership and to decide who will deal with the consequences, but also to prove that the actions taken will be beneficial for most (if not all) stakeholders.

The second potential drawback is directly related to the need of regional coordination that requires developing collaborative approaches and information sharing mechanisms. Communication is an important, and too often forgotten, phase of risk management. A process for improving the protection and resilience of critical infrastructure cannot be effective without considering the several stakeholders involved in critical infrastructure management and regional emergency management, including the public.

In risk management, it is always difficult to define what information must be communicated, to whom, and how. The development of processes that maintain a balance between protecting sensitive information (from a business and/or national security perspective) and providing emergency managers with necessary information continue to be a challenge.

Understanding regional security and safety capabilities is beneficial for harmonizing resilience strategies. However, an intelligent adversary can also use this information to exploit existing weaknesses. Identifying and admitting that your system can fail can also generate a loss of public confidence and affect critical infrastructure business activities. The difficulty to define what consequences are acceptable and what and how information should be shared can be addressed by building a trusted environment to promote a sustainable development culture based on education and training. The development of trust must be supported by mechanisms to operationalize standards and policies promoting collaborative approaches and partnerships between critical infrastructure owners/operators and government representatives. Furthermore, the objective of resilience management strategies is to complement risk management strategies, which primarily address threats and vulnerabilities, by promoting flexible and adaptive approaches to further reduce undesired consequences.

Resilience is a subset of risk specifically influencing the level of consequences resulting from detrimental events. Therefore, the implementation of resilience strategies is generally beneficial to decrease risk levels. However, all components of risk (i.e., threat, vulnerability, resilience, and consequence) are interdependent. For example, vulnerability and resilience are strongly related to the state of the system considered. Consequently, implementation of resilience strategies can affect the vulnerability levels. Resilience strategies are based on information sharing of vulnerabilities, protection and resilience measures, and regional capabilities, to lower the duration and importance of negative consequences. This can create additional vulnerabilities and therefore increase risk levels if this sensitive information is not protected and accessed by malicious people.

### Integrating critical infrastructure interdependencies in resilience management strategies

Assuring critical infrastructure continuity of operations requires to consider the complexity of their organization but also to understand the diversity of threats they could face. Critical infrastructure assets are part of a “system of systems” and cannot be considered independently of their operating environment.

As described by Rinaldi, Peerenboom, & Kelly (2001): “it is clearly impossible to adequately analyze or understand the behavior of a given infrastructure in isolation from the environment or other infrastructures”. These interconnections mean that disruption or failure of one element can lead to cascading failures in others. Interdependencies among infrastructure systems can result in important economic and physical damage on a citywide, regional, or even national or international scale. A critical infrastructure is thus in constant interaction with its environment, using and transforming inputs (i.e., critical services and resources) from the environment in order to provide outputs to the same environment. Several elements of its environment may directly affect the operations of a critical infrastructure, including economic and business opportunities and concerns, public policy, government investment decisions, legal and regulatory concerns, technical and security issues, social and political concerns, and public health and safety. (Rinaldi, Peerenboom, & Kelly, 2001)

The modern society faces an ongoing challenge of maintaining critical infrastructure performance and avoiding significant damage caused by extreme weather events (e.g. floods, earthquakes, hurricanes), manmade events (e.g., malevolence, terrorism), and aging equipment. As these events continue to increase in both frequency and intensity, the efforts of owners and operators to enhance the resilience of their systems are more crucial than ever. New technologies increase the complexity of assessing the resilience and security of critical infrastructure and the whole society. As a consequence, interdependency relationships among critical infrastructure assets and emerging threats must be characterized to anticipate how a change in these connections could affect critical infrastructure operations.

Based on the anticipation of what could constitute the future operating environment of critical infrastructure systems, the implementation of resilience strategies, by promoting coordination and collaboration at regional level, will help defining how critical infrastructure should modify (i.e., adapt or transform) their operations. Several approaches exist for defining security and resilience metrics but holistic risk and resilience assessments must go beyond traditional assessment approaches to integrate currently unknown threats in order to improve sustainability of today’s complex global systems (i.e., business, technology, society).

While organizational resilience and business continuity standards already exist, there is still a need to find new ways to anticipate and be prepared for emerging and hybrid threats but also to institutionalize security and resilience more holistically both nationally and internationally. Building codes and standards need to be enhanced to better integrate the concepts of resilience, define common terminology and protocols, propose indicators to compare and benchmark practices. Standardization approaches cannot be sectorial; it is necessary to emphasize community-scale issues in standardizing an approach to critical infrastructure and community resilience. Resilience standards should propose procedures for early recognition/identification and monitoring of emerging risks, and assessment framework for managing these new risks.

The challenge is to go beyond traditional risk management approaches based on historical data and to design critical infrastructure systems that will be adapted to their future socio-ecological environment and that will respond to current and future population needs.

**Annotated bibliography**

Carlson, L., Bassett, G., Buehring, W., Collins, M., Folga, S., Haffenden, B., Petit, F., Phillips, J., Verner, D., & Whitfield, R. (2012). Resilience: Theory and applications. Decision and Information Sciences Division, Argonne National Laboratory. Retrieved from https://publications.anl.gov/anlpubs/2012/02/72218.pdf. This report presents a brief overview of the emergence of resilience as an integral component of a comprehensive risk management strategy and consider definitions of resilience that have been proposed or applied in various areas. Based on a synthesis definition of resilience, the report also underlies the subsequent development and implementation of a set of instruments to measure resilience at both infrastructure and community levels. Finally, the reports identify resilience strategies that supported the development of resilience metrics and assessment methodologies currently used by the U.S. Department of Homeland Security.

Flynn, S. E. (2012). The New Homeland Security Imperative: The case for building greater societal and infrastructure resilience, Hearing on the future of Homeland Security: Evolving and emerging threats, Committee on Homeland Security and Governmental Affairs, U.S. Senate, Washington, DC, July 11, 2012. This document presents the testimony of Stephen Flynn in front of the U.S. Senate’s Committee on Homeland Security and Emerging Threats. This testimony specifically addresses the need to change the approach to Homeland Security by developing infrastructure and community resilience strategies.

Flynn, S. E. (2015). *Bolstering critical infrastructure resilience after superstorm sandy: Lessons for New York and the nation*. Boston, MA: Northeastern University. https://doi.org/10.17760/D20241717. This report presents lessons learned from the Superstorm Sandy event. In particular, it highlights the importance of developing community resilience strategies and better understanding how critical infrastructure systems operate.

National Academies of Sciences, Engineering, and Medicine. (2018). *The state of resilience: A leadership forum and community workshop, proceedings of a workshop*. Washington, DC: The National Academies Press. https://doi.org/10.17226/25054.This report presents the result of a workshop on community resilience. This workshop gave representatives from government agencies, private sector, and non-profit organizations the opportunity to discuss common issues and propose actions and solutions to build community resilience.

Petit, F., Verner, D., Brannegan, D., Buehring, W., Dickinson, D., Guziel, K., Haffenden, R., Phillips, J., & Peerenboom, J. (2015). Analysis of critical infrastructure dependencies and interdependencies. Decision and Information Sciences Division, Argonne National Laboratory. Retrieved from https://publications.anl.gov/anlpubs/2015/06/111906.pdf. This report presents the relationship between infrastructure dependencies, resilience, and risk. Based on elements characterizing infrastructure interdependencies, this report identifies a roadmap defining the four phases for developing a comprehensive and holistic interdependency assessment to enhance resilience strategies.

Petit, F., Verner, D., & Levy, L-A. (2017). Regional Resiliency Assessment Program Dependency Analysis Framework. Decision and Information Sciences Division, Argonne National Laboratory. Retrieved from https://publications.anl.gov/anlpubs/2018/04/137844.pdf. This report presents a framework to integrate infrastructure dependencies and interdependencies assessment in resilience management strategies. The U.S. Department of Homeland Security (DHS) Protective Security Coordination Division (PSCD) has adopted the assessment approach presented in this document to guide the consideration of infrastructure interdependencies in their Regional Resiliency Assessment Program (RRAP) projects.

## References

Carlson, J., Haffenden, R., Bassett, G., Buehring, W., Collins, M. I., Folga, S., Haffenden, R., Petit, F., Phillips, J., Verner, D., & Whitfield, R. (2012). Resilience: Theory and Application. Retrieved from https://www.osti.gov/biblio/1044521

U.S. Department of Homeland Security [DHS]. (2011). Presidential Policy Directive / PPD-8: National Preparedness. U.S. Department of Homeland Security. Retrieved from https://www.dhs.gov/presidential-policy-directive-8-national-preparedness

DHS. (2012). Office of Infrastructure Protection Strategic Plan: 2012–2016. Washington: U.S. Department of Homeland Security National Protection and Programs Directorate. Retrieved from https://www.dhs.gov/sites/default/files/publications/IP-Strategic-Plan-FINAL-508.pdf

DHS. (2013). NIPP 2013 - Partnering for Critical Infrastructure Security and Resilience. Washington: U.S. Department of Homeland Security. Retrieved from https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf

DHS. (2015). National Critical Infrastructure Security and Resilience Research and Development Plan. Washington: U.S. Department of Homeland Security. Retrieved from https://www.dhs.gov/sites/default/files/publications/National%20CISR%20R%26D%20Plan_Nov%202015.pdf

DHS. (2017). Regional Resiliency Assessment Program. Retrieved from U.S. Department of Homeland Security: https://www.dhs.gov/regional-resiliency-assessment-program

U.S. Department of Energy [DOE]. (2017). Quadrennial Energy Review - Transforming the Nation's Electricity System: The Second Instalment of the QER. Washington: U.S. Department of Energy. Retrieved from https://www.energy.gov/sites/prod/files/2017/02/f34/Quadrennial%20Energy%20Review--Second%20Installment%20%28Full%20Report%29.pdf

DOE. (2018). Grid Modernization Lab Consortium. Retrieved from U.S. Department of Energy: https://www.energy.gov/grid-modernization-initiative-0/grid-modernization-lab-consortium

Flynn, S. E. (2012). The New Homeland Security Imperative: The Case for Building Greater societal and Infrastructure Resilience. Retrieved from https://www.hsgac.senate.gov/imo/media/doc/Testimony-Flynn-2012-07-11-REVISED%201.pdf

Flynn, S. E. (2015). Bolstering Critical Infrastructure Resilience After Superstorm Sandy: Lessons for New York and the Nation. Retrieved from https://repository.library.northeastern.edu/files/neu:m0419677k

GMLC. (2017). Grid Modernization: Metrics Analysis (GMLC1.1) Reference Document Version 2.1. Washington: Grid Modernization Laboratory Consortium. Retrieved from https://gridmod.labworks.org/sites/default/files/resources/GMLC1%201_Reference_Manual_2%201_final_2017_06_01_v4_wPNNLNo_1.pdf

National Academies of Sciences. (2018). State of Resilience - A Leadership Forum and Community Workshop. Retrieved from https://www.nap.edu/catalog/25054/the-state-of-resilience-a-leadership-forum-and-community-workshop

NIAC. (2009). Critical Infrastructure Resilience - Final Report and Recommendations. Washington: National Infrastructure Advisory Council. Retrieved from https://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf

NIAC. (2010). A Framework for Establishing Critical Infrastructure Resilience Goals. Washington: National Infrastructure Advisory Council. Retrieved from https://www.dhs.gov/xlibrary/assets/niac/niac-a-framework-for-establishing-critical-infrastructure-resilience-goals-2010-10-19.pdf

Petit, F., Verner, D., & Levy, L.-A. (2017). Regional Resiliency Assessment Program Dependency Analysis Framework. Argonne: Argonne National Laboratory.

Petit, F., Verner, D., Brannegan, D., Buehring, W., Dickinson, D., Guziel, K., Haffenden, R., Phillips, J., & Peerenboom, J. (2015). Analysis of Critical Infrastructure Dependencies and Interdependencies. Retrieved from https://www.osti.gov/biblio/1184636-analysis-critical-infrastructure-dependencies-interdependencies

President's Commission on Critical Infrastructure Protection. (1997). Critical Foundations: Protecting America's Infrastructures. Washington: President's Commission on Critical Infrastructure Protection. Retrieved from https://fas.org/sgp/library/pccip.pdf

Rinaldi, S., Peerenboom, J., & Kelly, T. (2001). Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. IEEE Control Systems, 11-25.

The National Academies. (2012). Disaster Resilience A National Imperative. Washington: The National Academies Press. Retrieved from https://www.nap.edu/catalog/13457/disaster-resilience-a-national-imperative

The White House. (2013). Presidential Policy Directive/PPD-21 - Critical Infrastructure Security and Resilience. Retrieved from https://www.dhs.gov/sites/default/files/publications/PPD-21-Critical-Infrastructure-and-Resilience-508.pdf