Cyber Resilience Metrics: Key Observations

Deborah Bodeau, dbodeau@mitre.org
Richard Graubart, rdg@mitre.org
The MITRE Corporation

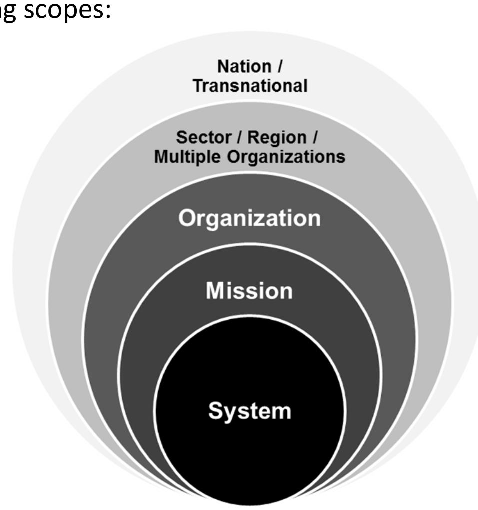
Abstract: As concern for cyber resilience grows, so does interest in metrics which can be used to compare alternatives or assess progress with respect to improving it. This point paper presents observations about cyber resilience metrics, drawn from experience, workshop sessions, and the literature, which could be helpful to those seeking to define cyber resilience metrics.

Introduction

Cyber resilience (or resiliency) is *the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources.*[1][2] Cyber resiliency can be a capability of a system, a system-of-systems, a mission, a business function, an organization, or a cross-organizational mission; the term can also be applied to an individual, household, group, region, or nation. The cyber resources, and the range of adversity to which cyber resources are susceptible, vary, depending on the context in which "cyber resilience" is sought. However, the potential for malicious cyber activities (MCA, [1]) to cause disruption is crucial to the understanding and assessment of cyber resilience.

As the need for ensuring cyber resilience increases, so does interest in defining, evaluating, and using metrics for cyber resilience, across the set of entities for which it is a desired capability. [2] For purposes of this white paper, cyber resilience is considered for the following scopes:

- Systems, including directed systems-of-systems (SoS);[3]
- Missions, including acknowledged SoS within an organization;
- Organizations, to which the CERT Resilience Management Model (RMM, [3]) or the DHS Cyber Resiliency Review (CRR, [4]) could be applied;
- Sectors (e.g., critical infrastructure sectors or sub-sectors), regions, and missions supported by multiple organizations, via collaborative SoS; and
- Nations and transnational enterprises supported by virtual SoS.



Note that systems, missions, and organizations are the three tiers considered in the multi-tiered approach to risk management defined in NIST SP 800-39 [5]. Experience with cyber resiliency analyses

[1] Cyber resources are "Separately manageable resources in cyberspace, including information in electronic form, as well as information systems, systems-of-systems, network infrastructures, shared services, and devices." (derived from NIST SP 800-39)
[2] This definition of cyber resilience is more general than, but is consistent with, the one given in [55]. It is designed to be consistent with national strategies and policies [56] [57], as well as with the DoD definition of operational resilience [68] and the definition used in resilience engineering [60] [58]. For simplicity of exposition, "adversity" will be used to include all forms of adverse conditions, stresses, attacks, or compromises.
[3] See [65] for a discussion of the types of SoS.

and assessments,[4] participation in workshop sessions,[5] and review of the literature on cyber resilience and metrics[6] enable us to make the following observations, which could be helpful to those seeking to define cyber resilience metrics.

General Observations

- *Cyber resilience* metrics relate primarily to the goals of withstanding or recovering from adverse conditions, disruption, stresses, attacks, or compromises. [6]
  - Metrics related to anticipating generally are attributed to contingency planning or cyber defense; metrics related to adapting generally are attributed to cyber defense or acquisition agility.[7]
  - Metrics related to recovering (and to a lesser extent on withstanding) can be construed in terms of reconstituting required capabilities. [7]
  - Metrics of availability in the face of disruption are not sufficient to measure cyber resilience, since they focus on a subset of the cyber resilience goals. In addition, many such metrics do not consider MCA as a source of disruption.
- *Evaluation* of cyber resilience metrics – like any metric evaluation – involves representation or assumption of characteristics of the environment in which resilience is sought. [8]
  - Evaluation environments can range from the highly situated and specific (e.g., a specific system in an operational context), to representative of a specific set of characteristics with others left unspecified (e.g., a cyber range, a modeling and simulation (M&S) environment), to conceptually representative (e.g., a tabletop exercise; an expert evaluation).
  - For system resilience, defining the system (and its boundaries) can be particularly challenging [9]; in a contested cyber environment, the system must be viewed as a socio-technical system which includes cyber defenders, mission users, and adversaries.
- A *single figure-of-merit* for resilience in general (and cyber resilience in particular) is often stated to be desirable, but proposed figures either obscure the complexity of the cyber resilience domain or require a large number of input measurements, which can vary so much in quality (e.g., timeliness, accuracy) that the resulting figure is highly uncertain.[8] [6]
  - To do justice to complexity, formulas and models that produce a single figure-of-merit represent large sets of possible adversities and potential consequences. [10] [11] [12] [13] [14] [15]

[4] See, for example, [59].
[5] The relationships between cyber security metrics, measures of effectiveness (MOEs), and cyber resiliency metrics were discussed in the Metrics and Assessment track of the 2012 Secure and Resilient Cyber Architectures Invitational [28]. Metrics related to cyber courses of action were discussed in the Active and Adaptive Response track of the 2013 Invitational [66]. The need for cyber resiliency metrics was also affirmed by the Systems Engineering Lifecycle track of the 2014 Invitational [67].
[6] An initial review was included in [6].
[7] Exceptions exist; for example, some (non-cyber) resilience metrics expressly consider adaptation [61].
[8] This is the case even when the figure-of-merit is ordinal: "… resilience is not a 1-dimensional quantity." [9] As captured in MITRE's Cyber Resiliency Engineering Framework (CREF, [55], updated in [25] and [63]), stakeholder goals and objectives, as well as the techniques that can be brought to bear to improve cyber resiliency, vary significantly depending on a number of political, operational, economic, and technical (POET) factors.

        - In M&S environments, these are tractable computationally and in terms of being able to supply input values of a consistent level of quality. [16] [17] [18] [19] [20] In addition, M&S enables determination of sensitivity to input values and assumptions.
        - Outside of M&S environments, complex formulas and models provide value as subjects of discussion among stakeholders and engineers, to clarify assumptions about what matters. Effectively, the formulas act as "boundary objects." [21] [22] [15] However, obtaining quality (e.g., timely, consistent) information at a reasonable cost presents significant challenges.
    - An alternative to a single figure-of-merit is the use of a set of indicators. [23] [14]
- *No single cyber resiliency metric or set of metrics* will work for all environments [24].
    - Defining a set of cyber resiliency metrics for a given system, class of systems, or mission needs to take into consideration the stakeholders whose decisions will be informed by the metrics, and their priorities and concerns. [6]
    - Evaluation of metrics has an associated cost – in terms of expert labor, and usually tools to gather and analyze data automatically. Therefore, the benefits of using the metrics need to be weighed against the costs of evaluation. [6]
    - Many security metrics – particularly those related to adversary activities at different points in the cyber attack lifecycle or cyber kill chain – can be repurposed as cyber resilience metrics, serving as indicators of cyber resilience capabilities. [6] [25] While repurposing security metrics can lower the costs of evaluation, care must be taken to avoid misinterpreting what the metrics actually indicate about cyber resilience. [6]

Observations about Cyber Resilience Metrics for Systems and Missions

- *System* cyber resilience metrics are either related to how well the system handles disruption, or to the system's architectural properties.
    - "*Disruption*" here means an event or set of circumstances that disrupts normal operations. Note that this includes not only degradation or denial of service, but also corruption of data, modification of services, and even unauthorized release of information (since the response to the detection of a data breach is often highly disruptive of normal operations).
        - Evaluation of cyber resilience metrics is highly sensitive to the disruption or set of disruptions considered.[9]
        - Restriction to a specific class of disruptions can make evaluation more tractable. [26]
        - For DoD systems, cyber resilience metrics related to disruption might be used in the definition of the System Survivability Key Performance Parameter (KPP) [27] and can be related to Measures of Effectiveness (MOEs) and Measures of Performance (MOPs) [28].
    - System cyber resilience metrics that reflect *architectural properties* are usually semi-quantitative (e.g., uses bins such as 0-15, 16-35, 36-70, 71-85, 86-100, or scales such as 1-

[9] "Given that the resilience of a system is so sensitive to the scenario under consideration, standardized scenarios being available for different problem spaces would allow the direct and reproducible comparison of different approaches to survivability (and robustness, and resilience) using different techniques. Without this, much of the work in resilient systems is open to criticism on the grounds that careful (or even random) selection of the scenario and requirements can lead to vastly different conclusions." [62]

10) or qualitative (e.g., very low, low, moderate, high, very high) in nature. [6] [14] Such metrics reflect Key System Attributes (KSAs) and/or cyber resiliency design principles.

        - For infrastructure systems, semi-quantitative metrics can be enhanced by performance metrics, which can be evaluated in M&S environments or in operational environments, using historical data. [29]

- Every cyber resilience metric related to disruption is a resilience metric, but not vice versa.
    - Metrics related to resilience in the face of non-adversarial threats generally measure whether, given a disruption, performance drops below an acceptable level and, if so, for how long it remains below that level. That is, resilience metrics measure some combination of "how much" and "for how long." [11]
        - "How much" can be expressed in terms of performance, capacity, or value delivery. [10]
    - Disruption-related metrics related to *cyber* resilience explicitly consider disruptions due to malicious cyber activities [30]. MCA can be stealthy (e.g., degrading performance but keeping it above the minimum acceptable level, actually improving performance to conceal such activities as data exfiltration) Disruptions due to MCA can be repeated or maintained at the adversary's direction. Consideration of MCA differentiates cyber resilience; the threat model for resilience metrics in other problem domains typically involves a discrete and discernable precipitating event.
        - One discriminator between a general and a cyber resilience metric is whether the metric could be used in adversarial testing.
        - Another discriminator is whether the metric relates clearly to a cyber resiliency objective or technique. [25]
        - Because cyber resilience metrics assume an adversary, "with how much confidence" can be a factor, along with "how much" and "for how long." [31]
    - Modeling and simulation (M&S) can be used to evaluate disruption-related metrics for systems, networks [17], systems-of-systems [16], and missions [18] [16].
- Resilience metrics are closely related to risk metrics [32]. The relationship between risk and resilience can be problematic, particularly in the complex (and socio-technical) systems considered in catastrophe management [33] [34].
    - However, the relationship can be usefully articulated in the case of *mission* resilience and *mission* risk [11].
    - Because *cyber* resilience is predicated on the assumption that compromises will occur, cyber resilience metrics focus on the consequence aspect of the conventional cyber security risk model (risk as a function of threat, vulnerabilities or predisposing conditions, and consequences).
        - Therefore, cyber resilience metrics depend on the ability to determine the cyber impacts of adversity. [35] [18] [19] [36]
- The definition of system resilience metrics needs to take the type of system into consideration, since the requirements for, types of disruptions that are most concerning, and possibilities for evaluation depend on whether the system is general-purpose information technology (IT),

operational technology (OT) or an industrial control system (ICS) [24], cyber-physical systems (CPS) in general [37], or a highly specialized CPS such as a medical device.

Observations about Cyber Resilience Metrics for Organizations and Beyond

- *Organizational* or *operational* resilience metrics are sought in the contexts of cybersecurity, contingency planning, and overall risk management [38].
  - At the level of reporting to a Corporate Board, metrics for risk and resilience are so closely associated that a single reporting mechanism is desirable. Qualitative values are often sufficient [38].
  - Organizational resilience metrics can be model-based, e.g., using the CERT Resilience Management Model (RMM) [39] or a maturity model [40]. However, the role of cyber resilience in models of organizational resilience is not well articulated, and often devolves to consideration of incident response.
    - The Cyber Resilience Review (CRR, [41]), derived from the RMM, is a "non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices." The CRR has been mapped to the NIST Cybersecurity Framework [42]. However, the NIST Cybersecurity Framework (NCF, [43]) does not fully address cyber resilience; for example, the Framework Core does not include many of the security controls in NIST SP 800-53R4 related to cyber resilience techniques [44]. Therefore, CRR-based (or NCF-based) organizational resilience metrics will not represent the full range of cyber resilience capabilities, opportunities, or gaps.
    - The idea of value-at-risk, originally defined in the financial services domain, has been adapted to the cyber domain, applied to an organization's assets and reputation [45]. The cyber value-at-risk model is tied to the idea of a maturity model [32], while acknowledging the lack of standardized models.
- *Sector* resilience metrics can be defined using a framework based on risk metrics, relying on a resilience analysis process. For the energy sector, see [46] for a survey of metrics at multiple scales and [47] for the recommended framework. However, estimating probability of consequence can be problematic for advanced cyber threats.
  - Sector *cyber* resilience metrics can be defined in terms of sector targets for reliability or availability (see [48] [49] for the financial sector). However, sector recovery time objectives can be problematic when applied to cyber attacks [50].
- The need for *regional* or *community* resilience metrics has been noted [51], and cyber resilience has been identified as a constituent of regional resilience [52]. However, complex interdependencies among organizations, systems, and critical infrastructures, as well as significant differences between preparedness and response for different types of disruptions, present major challenges to resilience assessment for regions or communities [53] [54].

References

[1] National Science and Technology Council, "Federal Cybersecurity Research and Development Strategic Plan," February 2016. [Online]. Available: https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/2016_Federal_Cybersecurity_Research_and_Development_Stratgeic_Plan.pdf.

[2] National Infrastructure Advisory Council (NIAC), "Critical Infrastructure Security and Resilience National Research and Development Plan: Final Report and Recommendations," 14 November 2014. [Online]. Available: http://www.dhs.gov/sites/default/files/publications/NIAC-CISR-RD-Plan-Report-508.pdf.

[3] CERT Program, "CERT® Resilience Management Model, Version 1.0: Improving Operational Resilience Processes," May 2010. [Online]. Available: http://www.cert.org/archive/pdf/10tr012.pdf.

[4] DHS, "Cyber Resilience Review Fact Sheet," 26 September 2014. [Online]. Available: https://www.dhs.gov/sites/default/files/publications/Cyber-Resilience-Review-Fact-Sheet-508.pdf.

[5] NIST, "NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View," March 2011. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf.

[6] D. Bodeau, R. Graubart, L. LaPadula, P. Kertzner, A. Rosenthal and J. Brennan, "Cyber Resiliency Metrics," April 2012. [Online]. Available: https://registerdev1.mitre.org/sr/12_2226.pdf.

[7] P. Ramuhalli, M. Halappanavar, J. Coble and M. Dixit, "Towards A Theory of Autonomous Reconstitution of Compromised Cyber-Systems," *Homeland Security Affairs, Supplement 6,* p. April, 2014.

[8] D. Bodeau, R. Graubart and W. Heinbockel, "Mapping the Cyber Terrain: Enabling Cyber Defensibility Claims and Hypotheses to Be Stated and Evaluated with Greater Rigor and Utility (MTR130433)," 2013. [Online]. Available: http://www.mitre.org/sites/default/files/publications/mapping-cyber-terrain-13-4175.pdf.

[9] R. Ford, M. Cavalho, L. Mayron and M. Bishop, "Toward Metrics for Cyber Resilience," in *21st EICAR (European Institute for Computer Anti-Virus Research) Annual Conference Proceedings*, 2012.

[10] O. Madaya, The Resilience of Networked Infrastructure Systems: Analysis and Measurement (Systems Research Series — Vol. 3), Hackensack, NJ: World Scientific Publishing Company, 2013.

[11] S. Musman and S. Agbolosu-Amison, "A Measurable Definition of Resiliency Using "Mission Risk" as a Metric," March 2014. [Online]. Available: http://www.mitre.org/sites/default/files/publications/resiliency-mission-risk-14-0500.pdf.

[12] D. G. Dessavre and J. E. Ramirez-Marquez, "Computational Techniques for the Approximation of Total System Resilience," in *Safety and Reliability of Complex Engineered Systems: ESREL 2015*, Zurich, Switzerland, 2015.

[13] L. Wang, S. Jajodia, A. Singhal and S. Noel, "k-Zero Day Safety: Measuring the Security Risk of Networks against Unknown Attacks," in *European Symposium on Research in Computer Security (ESORICS)*, Athens, Greece, 2010.

[14] S. Noel and S. Jajodia, "Metrics Suite for Network Attack Graph Analytics," in *9th Annual Cyber and Information Security Research Conference (CISRC)*, Oak Ridge National Laboratory, TN, 2014.

[15] S. Noel, S. Jajodia, L. Wang and A. Singhal, "Measuring Security Risk of Networks Using Attack Graphs," *International Journal of Next-Generation Computing,* vol. 1, no. 1, 2010.

[16] S. Hassell, R. Case, G. Ganga, S. R. Martin, S. Marra and C. Eck, "Using DoDAF and Metrics for Evaluation of the Resilience of Systems, Systems of Systems, and Networks Against Cyber Threats," *INCOSE Insight,* pp. 26-28, April 2015.

[17] P. Beraud, A. Cruz, S. Hassell and S. Meadows, "Using Cyber Maneuver to Improve Network Resiliency," in *MILCOM*, Baltimore, MD, 2011.

[18] S. Musman and A. Temin, "A Cyber Mission Impact Assessment Tool (PR 14-3545)," in *2015 IEEE International Symposium on Technologies for Homeland Security (HST)*, Waltham, MA, 2015.

[19] S. Noel, J. Ludwig, P. Jain, D. Johnson, R. K. Thomas, J. McFarland, B. King, S. Webster and B. Tello, "Analyzing Mission Impacts of Cyber Actions (AMICA), STO-MP-AVT-211," 1 June 2015. [Online]. Available: http://csis.gmu.edu/noel/pubs/2015_AMICA.pdf.

[20] S. Martin and S. Hassell, "Cyber Analysis Evaluation Modeling for Operations - Countering the Cyberthreat," 2013. [Online]. Available: Cyber Analysis Modeling Evaluation for Operations (CAMEO) — Countering the Cyberthreat - See more at: http://www.raytheon.com/newsroom/technology_today/2013_i1/cameo.html#sthash.gYtx3MKS.dpuf.

[21] G. C. Bowker and S. L. Star, Sorting Things Out: Classification and Its Consequences, The MIT Press, 1999.

[22] M. Albanese, S. Jajodia and S. Noel, "Time-Efficient and Cost-Effective Network Hardening Using Attack Graphs," in *42nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, Boston, MA, 2012.

[23] E. L. F. Schipper and L. Langston, "A comparative overview of resilience measurement frameworks: analysing indicators and approaches (ODI Working Paper 422)," July 2015. [Online]. Available: http://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/9754.pdf.

[24] Z. A. Collier, M. Panwar, A. A. Ganin, A. Kott and I. Linkov, "Security Metrics in Industrial Control Systems," in *Cyber Security of Industrial Control Systems, Including SCADA Systems*, New York, NY, Springer, 2016.

[25] D. Bodeau and R. Graubart, "Cyber Resiliency Assessment: Enabling Architectural Improvement (MTR 120407, PR 12-3795)," May 2013. [Online]. Available: http://www.mitre.org/sites/default/files/pdf/12_3795.pdf.

[26] G. A. Fink, R. L. Griswold and Z. W. Beech, "Quantifying cyber-resilience against resource-exhaustion attacks," in *7th International Symposium on Resilient Control Systems (ISRCS)*, Denver, CO, 2014.

[27] DoD, "Manual for the Operation of The Joint Capabilities Integration and Development System (JCIDS)," 12 February 2015. [Online]. Available: https://dap.dau.mil/policy/Documents/2015/JCIDS_Manual_-_Release_version_20150212.pdf.

[28] The MITRE Corporation (ed.), "2nd Secure and Resilient Cyber Architectures Workshop: Final Report," 2012. [Online]. Available: https://registerdev1.mitre.org/sr/2012_resiliency_workshop_report.pdf.

[29] E. D. Vugrin and J. Turgeon, "Advancing Cyber Resilience Analysis with Performance-Based Metrics from Infrastructure Assessment," in *Cyber Behavior: Concepts, Methodologies, Tools, and Applications*, Hershey, PA, IGI Global, 2014, pp. 2033-2055.

[30] DoD, "The Department of Defense Cyber Strategy," April 2015. [Online]. Available: http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

[31] S. Noel, E. Robertson and S. Jajodia, "Correlating Intrusion Events and Building Attack Scenarios through Attack Graph Distances," in *20th Annual Computer Security Applications Conference (ACSAC)*, Tucson, AZ, 2004.

[32] World Economic Forum, "Partnering for Cyber Resilience: Toward the Quantification of Cyber Risks," 19 January 2015. [Online]. Available: http://www3.weforum.org/docs/WEFUSA_QuantificationofCyberThreats_Report2015.pdf.

[33] J. Park, T. P. Seager, P. S. Rao, M. Convertino and I. Linkov, "Integrating risk and resilience approaches to catastrophe management in engineering systems," *Risk Analysis,* vol. 33, no. 3, pp. 356-367, 2013.

[34] I. Linkov, D. A. Eisenberg, M. E. Bates, D. Chang, M. Convertino, J. H. Allen, S. E. Flynn and T. P. Seager, "Measurable Resilience for Actionable Policy," *Environmental Science & Technology,* vol. 47, p. 10108−10110, 2013.

[35] Y. Cheng, J. Deng, J. Li, S. A. DeLoach, A. Singhal and X. Ou, "Metrics of Security," in *Cyber Defense and Situational Awareness, Advances in Information Security 62*, Springer International Publishing, 2014, pp. 263-265.

[36] H. Cam and P. Mouallem, "Mission-Aware Time-Dependent Cyber Asset Criticality and Resilience," in *Proceedings of the 8th CSIIRW Cyber Security and Information Intelligence Research Workshop*, Oak Ridge National Lab, Oak Ridge, TN, 2013.

[37] J. Zalewski, S. Drager, W. McKeever, A. J. Kornecki and B. Czejdo, "Modeling Resiliency and Its Essential Components for Cyberphysical Systems," in *Position Papers of the Federated Conference on Computer Science and Information Systems (FedCSIS)*.

[38] Council on Competitiveness, "Why Enterprise Resilience Matters," 2010. [Online]. Available: http://usresilienceproject.org/wp-content/uploads/2014/09/report-Prepare_Why_Enterprise-Resilience_Matters.pdf.

[39] J. Allen and N. Davis, "Measuring Operational Resilience Using the CERT® Resilience Management Model," September 2010. [Online]. Available: http://www.cert.org/archive/pdf/10tn030.pdf.

[40] World Economic Forum, "Partnering for Cyber Resilience: Risk and Responsibilities in a Hyperconnected World - Principles and Guidelines," March 2012. [Online]. Available: http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf.

[41] DHS, "Assessments: Cyber Resilience Review (CRR)," US-CERT, [Online]. Available: https://www.us-cert.gov/ccubedvp/assessments.

[42] DHS, "Cyber Resilience Review (CRR): NIST Cybersecurity Framework Crosswalk," February 2014. [Online]. Available: https://www.us-cert.gov/sites/default/files/c3vp/csc-crr-nist-framework-crosswalk.pdf.

[43] NIST, "Framework for Improving Critical Infrastructure Security, Version 1.0," 12 February 2014. [Online]. Available: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[44] D. Bodeau, Graubart and Richard, "Cyber Resiliency and NIST Special Publication 800-53 Rev.4 Controls (MTR 130531, PR 13-4037)," September 2013. [Online]. Available: http://www.mitre.org/sites/default/files/publications/13-4047.pdf.

[45] World Economic Forum, "Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience," 4 November 2014. [Online]. Available: http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf.

[46] H. H. Willis and K. Loa, "Measuring the Resilience of Energy Distribution Systems, RAND Justice, Infrastructure, and Environment, PR-1293-DOE," July 2014. [Online]. Available: http://www.rand.org/content/dam/rand/pubs/research_reports/RR800/RR883/RAND_RR883.pdf.

[47] J.-P. Watson, R. Guttromson, C. Silva-Monroy, R. Jeffers, K. Jones, J. Ellison, C. Rath, J. Gearhart, D. Jones, T. Corbet, C. Hanley and L. T. Walker, "Conceptual Framework for Developing Resilience Metrics for US Electricity, Oil, and Gas Sectors, SAND2014-18019," September 2015. [Online]. Available: http://energy.gov/sites/prod/files/2015/09/f26/EnergyResilienceReport_%28Final%29_SAND2015-18019.pdf.

[48] Committee on Payments and Market Infrastructures, Bank for International Settlements, "Cyber resilience in financial market infrastructures," November 2014. [Online]. Available: http://www.bis.org/cpmi/publ/d122.pdf.

[49] Committee on Payments and Market Infrastructures, Board of the International Organization of Securities Commissions, "Guidance on cyber resilience for financial market infrastructures - consultative report," November 2015. [Online]. Available: http://www.bis.org/cpmi/publ/d138.pdf.

[50] J. King, "DTCC's Bodson Discusses Cyber Resilience at World Economic Forum," Depository Trust and Clearing Corporation, 3 February 2016. [Online]. Available: http://www.dtcc.com/news/2016/february/03/dtccs-bodson-discusses-cyber-resilience.

[51] E. Frye, "Critical Infrastructure Resilience: A Regional and National Approach (PR 14-4047)," November 2014. [Online]. Available: http://www.mitre.org/sites/default/files/publications/14-4047-critical-infrastructure-resilience-a-regional-and-national-approach.pdf.

[52] P. Scalingi, "Operationalizing Bay Area Disaster Resilience: Status, Challenges, and Opportunities (presentation)," 11 September 2014. [Online]. Available: http://www.samesanfrancisco.org/wp-content/uploads/2014/09/SAME_SFP_Meeting_Sept2014.pdf.

[53] J. H. Kahan, "Resilience Redux: Buzzword or Basis for Homeland Security," *Homeland Security Affairs Journal,* vol. 11, no. 2, February 2015.

[54] L. Carlson, G. Bassett, W. Buehring, M. Collins, S. Folga, B. Haffenden, F. Petit, J. Phillips, D. Verner and R. Whitfield, "Resilience: Theory and Applications (ANL/DIS-12-1)," January 2012. [Online]. Available: http://www.ipd.anl.gov/anlpubs/2012/02/72218.pdf.

[55] D. Bodeau and R. Graubart, "Cyber Resiliency Engineering Framework (MTR110237, PR 11-4436)," September 2011. [Online]. Available: http://www.mitre.org/sites/default/files/pdf/11_4436.pdf.

[56] Office of the President, "National Security Strategy," May 2010. [Online]. Available: https://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

[57] Office of the President, "Presidential Policy Directive (PPD) 21 -- Critical Infrastructure Security and Resilience," 12 February 2013. [Online]. Available: http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[58] A. M. Madni and S. Jackson, "Towards a Conceptual Framework for Resilience Engineering," *IEEE Systems Journal, Vol. 3, No. 2,* June 2009.

[59] D. J. Bodeau, "Analysis Through a Resilience Lens: Experiences and Lessons-Learned (PR 15-1309) (presentation)," in *5th Annual Secure and Resilient Cyber Architectures Invitational*, McLean, VA, 2015.

[60] INCOSE, "Resilience Engineering," in *INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities, Fourth Edition*, Hoboken, NJ, John Wiley & Sons, 2015, pp. 229-231.

[61] O. Erol, H. Devanandham and B. Sauser, "Exploring Resilience Measurement Methdologies," in *INCOSE International Symposium*, Chicago, IL, 2010.

[62] R. Ford, M. Cavalho, L. Mayron and M. Bishop, "Antimalware Software: Do We Measure Resilience?," in *2013 Workshop on Anti-malware Testing Research (WATeR)*, Montreal, Quebec, 2013.

[63] D. Bodeau, R. Graubart, W. Heinbockel and E. Laderman, "Cyber Resiliency Engineering Aid-The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques, MTR140499R1, PR 15-1334," May 2015. [Online]. Available: http://www.mitre.org/sites/default/files/publications/pr-15-1334-cyber-resiliency-engineering-aid-framework-update.pdf or http://www.defenseinnovationmarketplace.mil/resources/20150527_Cyber_Resiliency_Engineering_Aid-Cyber_Resiliency_Techniques.pdf.

[64] M. Pendleton, R. Garcia-Lebron and S. Xu, "A Survey on Security Metrics," 20 January 2016. [Online]. Available: http://arxiv.org/pdf/1601.05792v1.pdf.

[65] D. Bodeau, J. Brtis, R. Graubart and J. Salwen, "Resiliency Techniques for System of Systems: Extending and Applying the Cyber Resiliency Engineering Framework to the Space Domain (MTR 130515, PR 13-3513)," September 2013. [Online]. Available: http://www.mitre.org/sites/default/files/publications/13-3513-ResiliencyTechniques_0.pdf.

[66] The MITRE Corporation (ed.), "Third Annual Secure and Resilient Cyber Architectures Workshop," December 2013. [Online]. Available: http://www.mitre.org/sites/default/files/publications/13-4210.pdf.

[67] The MITRE Corporation (ed.), "Fourth Annual Secure and Resilient Cyber Architectures Invitational," 2015. [Online]. Available: http://www.mitre.org/sites/default/files/pdf/2014-Secure-Resilient-Cyber-Architectures-Report-15-0704.pdf.

[68] DoD CIO, "DoDI 8500.01, Cybersecurity," 14 March 2014. [Online]. Available: http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf.