Cyber Resiliency Resource List

Cyber resiliency (also referred to as cyber resilience) is *the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources*. (This definition has evolved over time; thus, many of the resources identified below present alternative definitions.)

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 entity for which "cyber resilience" is sought. In any situation, the underlying assumption is that the entity to be made cyber resilient depends on cyber resources to do something, and that "adverse conditions, stresses, attacks, or compromises" create risk due to that dependence.

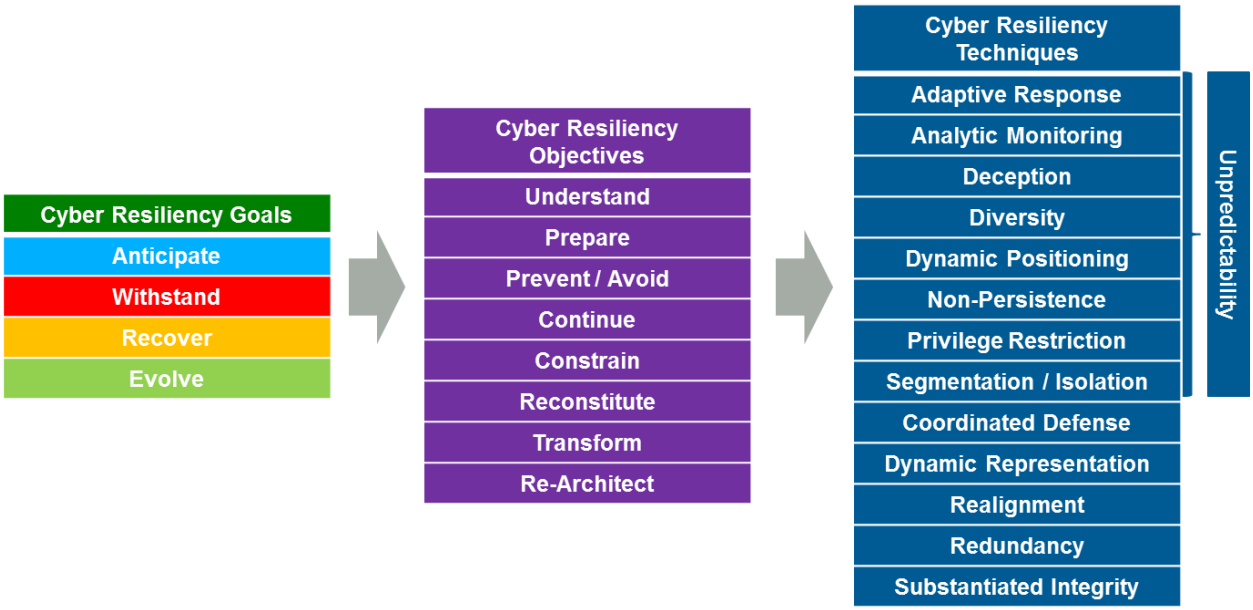
Since 2010, The MITRE Corporation has been active in defining, promulgating, and bringing together stakeholders in cyber resiliency frameworks, methodologies, metrics, and tools. In response to a recommendation from participants at the 2015 Secure and Resilient Cyber Architectures Invitational, MITRE has assembled this list of resources.

MITRE's Publicly Released White Papers

MITRE's publicly released white papers include the initial definition and subsequent refinement of the Cyber Resiliency Engineering Framework, materials on cyber resiliency metrics and assessment, and relationships between cyber resiliency and other concepts and processes.

Cyber Resiliency Engineering Framework

The Cyber Resiliency Engineering Framework (CREF) illustrated below organizes the cyber resiliency domain into a set of goals, objectives, and techniques.



The initial version of the CREF [1] was published in 2011:
http://www.mitre.org/sites/default/files/pdf/11_4436.pdf

Additional discussion of cyber resiliency techniques can be found in the 2012 Assessment paper at http://www.mitre.org/sites/default/files/pdf/12_3795.pdf .

The current version of the CREF is in the 2015 Cyber Resiliency Engineering Aid [2]: http://www.mitre.org/sites/default/files/publications/pr-15-1334-cyber-resiliency-engineering-aid-framework-update.pdf. This version

- Updates and supersedes an earlier Engineering Aid,
- Incorporates material on representative approaches to implementing the cyber resiliency techniques originally defined for systems-of-systems [3]: http://www.mitre.org/sites/default/files/publications/13-3513-ResiliencyTechniques_0.pdf, and
- Provides assessments of the overall maturity and adoption of those approaches, and incorporates material from the paper on effects of cyber resiliency techniques on adversary activities identified below.

Note that while the Cyber Resiliency Engineering Aid provides the most current version of the CREF, it presents a more complicated version of the definition of cyber resiliency.

Cyber Resiliency Metrics and Assessment

The initial version of the CREF was accompanied by a white paper on cyber resiliency metrics [4]: https://registerdev1.mitre.org/sr/12_2226.pdf.

A point paper presenting observations on cyber resiliency metrics, based on experience, recent literature, and workshop discussions [5]: https://www.mitre.org/sites/default/files/publications/pr-16-0779-cyber-resilience-metrics-key-observations.pdf. A longer paper [6] discusses the relationship between cyber resiliency and mission risk in more detail: http://www.mitre.org/sites/default/files/publications/resiliency-mission-risk-14-0500.pdf.

A paper on performing cyber resiliency architectural assessments was published in 2013 [7]: http://www.mitre.org/sites/default/files/pdf/12_3795.pdf. This document includes extensive discussion of cyber resiliency techniques, including identification of POET (political, operational, economic, and technical) factors that could affect the adoption of those techniques. A short paper on cyber resiliency assessments provides an overview [8]: https://registerdev1.mitre.org/sr/cyber_engineering.pdf.

An updated overview paper describes the Structured Cyber Resiliency Analysis Methodology (SCRAM), which has been used to perform cyber resiliency analyses with varying scopes and purposes, at different points in the lifecycle of a system, system-of-systems, or mission [9]: https://www.mitre.org/sites/default/files/publications/pr-16-0777-structured-cyber-resiliency-analysis-methodology-overview.pdf

Cyber Resiliency in Relationship to Other Concepts and Processes

Research

A snapshot of the cyber resiliency research landscape was published in 2011 [10]: http://www.mitre.org/sites/default/files/pdf/11_3023.pdf

Definitions

The definition of cyber resiliency MITRE uses – *the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources* – is derived from definitions of resilience and resiliency used by different communities of interest. The initial CREF document provides a survey of definitional sources, and relationships to such concepts as survivability and fault tolerance. Sources of definitions of operational resilience, or resilience in the context of national security or critical infrastructure protection, not cited in the initial CREF document include

- PPD-21 [11], Presidential Policy Directive-21, *Critical Infrastructure Security and Resilience,* February 12, 2013. https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
- DoDI 8500.01 [12], Cyber Security, March 14, 2014. http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf

Security Controls and the Risk Management Framework

NIST SP 800-53R4 [13] includes security controls that support cyber resiliency. These were identified in 2013, using an earlier version of the CREF [14]: http://www.mitre.org/sites/default/files/publications/13-4047.pdf. An updated version of this material can be found in the Second Public Draft of NIST SP 800-160 ([15], see below). A discussion of the relationship between cyber resiliency and the risk management framework (RMF) [16] can be found at https://www.mitre.org/sites/default/files/publications/pr-16-0776-cyber-resiliency-and-the-risk-management-framework.pdf.

Effects Against Adversary Activities

One way to analyze the potential effectiveness of cyber resiliency measures (technologies, processes, architectural decisions, or specific technical or procedural solutions) is to consider the effects those measures could have on adversary activities. A vocabulary for describing effects on adversary activities is defined and applied to cyber resiliency techniques [17]: http://www.mitre.org/sites/default/files/publications/characterizing-effects-cyber-adversary-13-4173.pdf. An updated version of that vocabulary is presented in the Cyber Resiliency Engineering Aid, and is applied to the representative approaches to implementing cyber resiliency techniques.

Secure and Resilient Cyber Architectures (S&RCA) Invitational events

The purpose of the MITRE-hosted series of Secure and Resilient Cyber Architectures Invitational events (originally referred to as workshops) is to accelerate recognition and adoption of cyber resilience by bringing together the cyber resiliency community for collective work on topics of common concern. The first workshop in October 2010 established the initial community and shared architectural, technical, and policy perspectives on cyber resiliency. The second workshop, held in May 2012, focused on collaborating to develop a communal view of resiliency frameworks, engineering principles, and metrics. The third annual workshop, held in June 2013, focused on identifying favorable conditions for use of specific resiliency techniques, assessing the use of techniques in enterprise architectures, and developing use cases. The fourth annual Invitational, held in May 2014, focused on applying cyber resilience to space and critical infrastructure, designing a cyber resilience challenge, and identifying roles played by cyber resilience throughout the systems engineering life cycle. The Fifth Annual Secure and

Resilient Cyber Architectures Invitational, held in May 2015, focused on taking stock of the state of cyber resiliency – what lessons have been learned and what challenges still need to be overcome.

- Initial thought paper by Harriet Goldman [18]: http://www.mitre.org/sites/default/files/pdf/10_3301.pdf
- Report of the Second Annual Secure and Resilient Cyber Architectures Workshop [19]: https://registerdev1.mitre.org/sr/2012_resiliency_workshop_report.pdf
- Report of the Third Annual Secure and Resilient Cyber Architectures Workshop [20]: http://www.mitre.org/sites/default/files/publications/13-4210.pdf
- Report of the Fourth Annual Secure and Resilient Cyber Architectures Invitational [21]: http://www.mitre.org/sites/default/files/pdf/2014-Secure-Resilient-Cyber-Architectures-Report-15-0704.pdf
- Report of the Fifth Annual Secure and Resilient Cyber Architectures Invitational (forthcoming)

Key Cyber Resiliency and Related Initiatives and Resources

Four key initiatives related to cyber resiliency have had a strong presence at the Secure and Resilient Cyber Architectures Invitationals: the inclusion of a system resiliency appendix in the Second Public Draft of NIST SP 800-160, the CERT Resilience Management Model, the Asymmetric Resilient Cybersecurity (ARC) initiative at Pacific Northwest National Laboratory (PNNL), and a Government-industry collaboration.

System Resiliency Appendix in Second Public Draft of NIST SP 800-160

Appendix H of the Second Public Draft of NIST SP 800-160, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* [15], provides guidance on integrating resiliency techniques into the systems engineering process: http://csrc.nist.gov/publications/drafts/800-160/sp800_160_second-draft.pdf.

The expository material in Appendix H is consistent with the current version of the CREF. In addition to describing a framework for system resiliency, discussing potential effects on threat events and risk, and discussing factors to consider when selecting resiliency techniques and approaches for a system, Appendix H identifies approximately 150 security controls and control enhancements in NIST SP 800-53R4 which map to resiliency techniques. That mapping updates [14].

CERT Resilience Management Model

The CERT Resilience Management Model (RMM™, [22]) provides a framework for defining and improving organizational or operational resilience: http://www.cert.org/resilience/products-services/cert-rmm/.

The CERT RMM has been applied to the problem of organizational resilience against cyber threats, initially in the context of the electrical sector via the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2, [23]): http://energy.gov/sites/prod/files/Electricity%20Subsector%20Cybersecurity%20Capabilities%20Maturity%20Model%20(ES-C2M2)%20-%20May%202012.pdf.

The ES-C2M2 was used as the basis for the DHS Cyber Resilience Review (CRR, [24]): https://www.us-cert.gov/ccubedvp/assessments.

Asymmetric Resilient Cybersecurity at PNNL

The Asymmetric Resilient Cybersecurity (ARC, [25]) initiative is developing theory, processes, methodologies, and algorithms that will enable a resilient cyber infrastructure with an asymmetric advantage to thwart adversaries: http://cybersecurity.pnnl.gov/arc.stm.

Multiple projects are active under the ARC initiative: http://cybersecurity.pnnl.gov/projects.stm.

Resilience Research at the US Army Engineer Research and Development Center

Resilience research at the US Army Engineer Research and Development Center considers resilience in a broader context than cyberspace, applying concepts related to risk analysis and environmental modeling [26] [27]. Central to that work is the observation that systems exist in four domains: physical, information, cognitive, and social. That work has been applied to the cyber domain [28] [29], including to network centric operations [30] and industrial control systems [31].

Government-Industry Collaboration

A collaboration with Government and commercial organizations [32] identified best practices for six activities "pre-bang" (i.e., prior to a cyber incursion), for six activities "post-bang," and for disrupting the attack surface. Those practices include design principles which restate and amplify the general statements of CREF-based techniques, in the context of enterprise information technology (IT). Many of these design principles focus on organizational processes, and thus are highly relevant to as-built systems.

Resources developed by this collaboration can be found at: http://www2.mitre.org/public/industry-perspective/index.html

Additional Cyber Resilience Initiatives and Resources

"Resilience" and "resiliency" are alternative spellings, with "resilience" being more common. The term "cyber resiliency" was chosen for MITRE's Cyber Resiliency Engineering Framework (CREF, [1] [7] [2]), to avoid creating the impression that cyber resiliency engineering was simply resilience engineering with "cyber" as a modifier. Cyber resiliency engineering draws upon resilience engineering, as demonstrated by the CREF goals, but also draws from cybersecurity and survivability, and explicitly addresses advanced cyber threats.

Since the publication of the CREF, the term "cyber resilience" has gained use, but is often being used to refer to organizational resilience against cyber threats, with a strong emphasis on effective implementation of good cybersecurity practices (e.g., using the NIST Cybersecurity Framework (CSF) [33]) and application of continuity of operations planning (COOP). In particular, the DHS Cyber Resilience Review (CRR, [24]), which is based on the CERT RMM, focuses on good cybersecurity practices, with an emphasis on conventional adversaries.

This section captures information about initiatives and resources related to cyber resilience. Unless specifically noted, these initiatives do not provide an explicit definition of cyber resilience.

The **Global Forum to Advance Cyber Resilience** [34], an initiative of the Global Institute for Cybersecurity and Research (GICSR), held its inaugural meeting February 16, 2016. The forum's focus is on critical infrastructure cyber resilience. The forum did not define the term "cyber resilience," but

Charlie Tupitza, Forum co-chair noted the importance of focusing on "how we can recover quickly from incidents that will occur while minimizing their effect. This includes cyber attacks and all types of incidents getting in the way of the organization to perform its mission." [35] The initiative plans to make use of the proprietary RESILIA™ best practices.

> **RESILIA**™ is "a portfolio of training, learning and certification aimed at building Cyber Resilience across the organization, from the boardroom down." [36] RESILIA is based on a Best Practice Guide, aligned with the ITIL® framework. It emphasizes the need to balance protect, detect, and correct; people, processes, and technology; and risks and opportunities [37].

The **National Academies of Sciences, Engineering, and Medicine** define resilience as "ability to prepare and plan for, absorb, respond, recover from, and more successfully adapt to adverse events." [38] The National Academies have multiple activities aimed at improving individual, community, and national resilience. One of these is the **Forum on Cyber Resilience** [39]. Themes addressed by the Forum include:

- "traditional notions of cybersecurity and trustworthiness, such as maintaining security in the face of attacks, resistance to degradation, and the ability to recover from adverse events,
- ways to foster resilience in the face of natural and man-made disasters, disruptive technological change, and diverse and dynamic user populations,
- how to sustain capacity for innovation and adaptation, and
- ways to reflect the values—such as privacy, openness, trust, expression, usability, dignity, access—and needs of many stakeholders." [40]

The **World Economic Forum** maintains a project, "**Partnering for Cyber Resilience**." "As an additional dimension of cyber risk management, "cyber resilience" is defined as the ability of systems and organizations to withstand cyber events, measured by the combination of mean time to failure and mean time to recovery." [41] The project has identified principles and guidelines, recognizing that organizations operate in "a hyperconnected world" [42], and has defined a maturity model for organizational cyber resilience. In addition, the project has identified an approach to quantifying cyber threats and risks, which defines "Cyber Value-at-Risk" (Cyber VAR) [43].

The **Chief Risk Officer (CRO) Forum** has published a paper on practical steps for cyber resilience, and the role of insurance [44]. That paper identifies four pillars of enhanced risk management: Prepare, Protect, Detect, and Improve. The CRO Forum explicitly recognizes the advanced persistent threat, and refers to the World Economic Forum work.

The Committee on Payments and Market Infrastructures, **Bank of International Settlements (BIS)**, developed a paper, *Cyber Resilience in Financial Market Infrastructures*, which reflected the 2014 understanding of FMI participants of the ability of their organizations, and of the financial system as a whole, to ensure the correct and timely operation of transactions despite the activities of adversarial actors in cyberspace [45]. The focus for FMI is on resuming operations within two hours. A more recent white paper, *Guidance on cyber resilience for financial market infrastructures* [46], defines four key functions for cyber resilience against disruptive cyber attacks: Identify, Protect, Detect, and Recover. (The white paper defines cyber resilience as "An FMI's ability to anticipate, withstand, contain and rapidly recover from a cyber attack.") While these functions correspond to the NIST Cybersecurity Framework (with Recover including both Respond and Recover), the white paper identifies four other components of cyber resilience: governance, testing, situational awareness, and learning and evolving.

Bibliography

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] D. Bodeau and R. Graubart, "Cyber Resiliency Metrics: Key Observations (PR Case No. 16-0779)," May 2016. [Online]. Available: https://www.mitre.org/publications/technical-papers/cyber-resiliency-metrics-key-observations.

[6] 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.

[7] 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.

[8] The MITRE Corporation, "Cyber Resiliency Engineering: An Overview of the Assessment Process," May 2013. [Online]. Available: https://registerdev1.mitre.org/sr/cyber_engineering.pdf.

[9] D. Bodeau and R. Graubart, "Structured Cyber Resiliency Analysis Methodology (SCRAM) (PR Case No. 16-0777)," May 2016. [Online]. Available: https://www.mitre.org/publications/technical-papers/structured-cyber-resiliency-analysis-methodology.

[10] R. Pietravalle and D. Lanz, "Resiliency Research Snapshot (PR Case No. 11-3023)," June 2011. [Online]. Available: http://www.mitre.org/work/tech_papers/2011/11_3023/11_3023.pdf.

[11] 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.

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

[13] NIST, "Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53 R4)," April 2013. [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.800-53r4.

[14] 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.

[15] NIST, "NIST SP 800-160 (Second Public Draft), Systems Security Engineering: A Multidisciplinary Approach to Building Trustworthy Secure Systems," 4 May 2016. [Online]. Available: http://csrc.nist.gov/publications/drafts/800-160/sp800_160_second-draft.pdf.

[16] R. Graubart and D. Bodeau, "The Risk Management Framework and Cyber Resiliency (PR Case No. 16-0776)," May 2016. [Online]. Available: https://www.mitre.org/publications/technical-papers/the-risk-management-framework-and-cyber-resiliency.

[17] D. Bodeau and R. Graubart, "Characterizing Effects on the Cyber Adversary: A Vocabulary for Analysis and Assessment (MTR 130432, PR 13-4173)," November 2013. [Online]. Available: http://www.mitre.org/sites/default/files/publications/characterizing-effects-cyber-adversary-13-4173.pdf.

[18] H. Goldman, "Building Secure, Resilient Architectures for Cyber Mission Assurance," 2010. [Online]. Available: http://www.mitre.org/sites/default/files/pdf/10_3301.pdf.

[19] 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.

[20] 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.

[21] 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.

[22] R. A. Caralli, J. H. Allen, D. W. White, L. R. Young, N. Mehravari and P. D. Curtis, "CERT® Resilience Management Model, Version 1.2," February 2016. [Online]. Available: http://www.cert.org/downloads/resilience/assets/cert-rmm-v1-2.pdf.

[23] DOE, "Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), Version 1.1," February 2014. [Online]. Available: http://energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf.

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

[25] PNNL, "Asymmetric Resilient Cybersecurity," Pacific Northwest National Laboratory, 2016. [Online]. Available: http://cybersecurity.pnnl.gov/arc.stm.

[26] 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.

[27] A. A. Ganin, E. Massaro, A. Gutfraind, N. Steen, J. M. Keisler, A. Kott, R. Mangoubi and I. Linkov, "Operational resilience: concepts, design and analysis," Nature.com Scientific Reports, 19 January 2016. [Online]. Available: http://www.nature.com/articles/srep19540.

[28] Z. A. Collier, I. Linkov and J. H. Lambert, "Four domains of cybersecurity: a risk-based systems approach to cyber decisions," *Environmental Systems & Decisions,* vol. 33, no. 4, pp. 469-470, 2013.

[29] I. Linkov, D. A. Eisenberg, K. Plourde, T. P. Seager, J. Allen and A. Kott, "Resilience metrics for cyber systems," *Environment Systems & Decisions,* vol. 33, no. 4, pp. 471-476, 2013.

[30] Z. A. Collier and I. Linkov, "Decision Making for Resilience within the Context of Network Centric Operations," in *19th Annual International Command and Control Research and Technology Symposium (19th ICCRTS)*, Alexandria, VA, 2014.

[31] 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; Advances in Information Security, Volume 66*, Springer, 2016.

[32] The MITRE Corporation, "Industry Perspective on Cyber Resiliency (home page)," Industry Perspective on Cyber Resiliency, 2015. [Online]. Available: http://www2.mitre.org/public/industry-perspective/index.html.

[33] 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.

[34] GICSR, "The Global Forum to Advance Cyber Resilience," Global Institute for Cybersecurity and Research, 2016. [Online]. Available: http://www.gicsr.org/gfacr/.

[35] R. Mullikin, "The Global Forum to Advance Cyber Resilience Holds Inaugural Meeting at the Kogod Cybersecurity Governance Center, February 18, 2016," PRWeb, 25 February 2016. [Online]. Available: http://www.prweb.com/releases/2016/02/prweb13235091.htm.

[36] Axelos, "RESILIA Best Practice Solutions for Cyber Resilience," Axelos, 2015. [Online]. Available: https://www.axelos.com/best-practice-solutions/resilia.

[37] S. Rance, "RESILIA™ Cyber Resilience Best Practices – in 3 minutes," Van Haren Publishing, 27 August 2015. [Online]. Available: http://www.vanharen.net/blog/it-management/resilia-cyber-resilience-best-practice/.

[38] The National Academies, "Resilience @ the Academies," The National Academies of Sciences, Engineering, and Medicine, [Online]. Available: http://www.nationalacademies.org/topics/resilience/index.html.

[39] Forum on Cyber Resilience, "The Forum on Cyber Resilience, a National Academies roundtable," The National Academies of Sciences, Engineering, and Medicine, 2016. [Online]. Available: http://sites.nationalacademies.org/DEPS/CYBER/index.htm.

[40] Forum on Cyber Resilience, "2015 Annual Report of Activities," 15 March 2016. [Online]. Available: http://sites.nationalacademies.org/cs/groups/depssite/documents/webpage/deps_171422.pdf.

[41] 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.

[42] 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.

[43] 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.

[44] CRO Forum, "Cyber resilience: The cyber risk challenge and the role of insurance," December 2014. [Online]. Available: http://www.thecroforum.org/wp-content/uploads/2014/12/Cyber-Risk-Paper-version-24.pdf.

[45] 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.

[46] Bank for International Settlements and International Organization of Securities Commissions, "Guidance on cyber resilience for financial market infrastructures," June 2016. [Online]. Available: https://www.bis.org/cpmi/publ/d146.pdf.