Application of Resilience Theory to Organizations Subject to Disinformation Campaigns

Amanda Wachtel
Sandia National Laboratories
Albuquerque, USA
awachte@sandia.gov

Susan Caskey
Sandia National Laboratories
Albuquerque, USA
sacaske@sandia.gov

Thushara Gunda
Sandia National Laboratories
Albuquerque, USA
tgunda@sandia.gov

Elizabeth Kistin Keller
Sandia National Laboratories
Albuquerque, USA
ejkisti@sandia.gov

2022 Resilience Week (RWS) | 978-1-6654-8819-8/22/$31.00 ©2022 IEEE | DOI: 10.1109/RWS55399.2022.9984033

***Abstract*—Community, corporate, and government organizations are being targeted by disinformation attacks at an unprecedented rate. These attacks interrupt the ability of organizations to make high-consequence decisions and can lower their confidence in datasets and analytics. New interdisciplinary research approaches are being actively developed to expand resilience theory applications to organizations, and to determine the metrics and mitigations needed to increase resilience against disinformation. This paper presents initial ideas on adapting resilience methodologies for organizations and disinformation, highlighting key areas that require further exploration in this emerging field of research.**

Keywords—resilience, metrics, disinformation, organizations

I. Introduction

For over a decade, researchers have been analyzing the resilience of energy and infrastructure systems to various threat types, including natural disasters, man-made attacks, and accidents [1]. For the purposes of this paper, resilience is defined following the Presidential Policy Directive-21 (PPD-21) as "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions" [2]. Through this extensive work, many quantitative frameworks have been developed to capture resilience theory for specific applications and at-large. While natural disasters and cyber-attacks remain at the forefront of infrastructure resilience planning, another threat is quickly overwhelming systems and society—disinformation. This research focuses on expanding current resilience theory applications to analyze organizations' resilience to disinformation attacks and provide insight into the levers organizations can use to increase resilience and continue to make high-quality, data-based decisions. Specifically, we start with a literature summary of different research fields relevant to this work and then present initial ideas on how scoping, modeling, and evaluation aspects of resilience methodologies would need to be adapted for organizations and disinformation. We conclude with key areas that require further exploration in this emerging field of research.

II. Relevant Research Domains

Three fields of research are brought together in this study: 1) the evaluation of disinformation impacts, 2) organizational resilience, and 3) infrastructure resilience, all of which have elements needed for organizational resilience to disinformation analysis (ORDA), but none of which fully address all aspects. For example, research about the spread of disinformation campaigns through social media looks at how information propagates across different groups, using network techniques to identify sources and bots [3] as well as influential actors [4]. While disinformation dispersed by social media may impact members of an organization and affect their worldview, the operations of an organization are governed by more complex interactions and processes that differ from general public engagements on social media platforms. Thus, limited insights can be gained from use of standard social media metrics (e.g., number of likes or shares) for evaluating disinformation attacks that are directly aimed at an organization that can affect the organization's ability to make critical decisions and/or take decisive action.

The second field of research relevant to this work focuses on organizational resilience at-large. Some commonly cited attributes of organizational resilience, as summarized nicely in [5], are situational awareness, managing vulnerabilities, having resources, the ability to improvise, the ability to anticipate events, agility, robustness, redundancy, flexibility, collaboration, learning capacity, and resilience of individuals. Many of these metrics might be applicable for evaluating disinformation threats against organizations. However, to date, this research is largely qualitative and thus, faces limitations for use in ORDA.

In contrast, the third field of research, energy and infrastructure resilience analysis, has contributed many quantitative metrics to support resilience assessments [6]. However, these methods have not focused on organizations beyond a basic understanding of whether or not an organization still has a source of power (when the impact of a threat is grid outages) or is suffering the consequences of a direct attack (such as a physical or cyber-attack). Such analyses focus primarily on impact to systems, and at best include human interactions with these systems as a secondary measure. However, the threat disinformation poses to organizations heavily impacts the decision-making process of those organizations and is therefore inextricably tied to human processes, not just technological systems, though those too may be affected.

III. Framing Organizational Resilience to Disinformation

The ORDA framework leverages Sandia's Integrated Methodology for Energy and Infrastructure Resilience Analysis [6]. Although this methodology was originally designed for energy and infrastructure applications, our team believes the general concepts can be adapted and applied to disinformation attacks against organizations. In particular, this methodology describes the main steps of a threat-informed, consequence-focused, and performance-based resilience analysis, which can be customized based on specific applications. These steps focus on: 1) scope and goals, 2) metrics, 3) baseline analysis, 4) mitigations, and 5) improvement analysis. The remainder of this section will go through these resilience analysis steps in greater detail, highlighting how they can be customized for ORDA (Fig. 1).

A. Scope and Goals

The first step of the ORDA framework is related to the scope and goals of the analysis, including defining the system, identifying threats, and categorizing resilience goals.

For this research, the systems of interest are organizations. We are specifically looking at organizations that are analyzing and using data to make decisions of consequence. These organizations may be small or large and may potentially be geographically distributed with multiple locations. Thus, structural variations of organizations for ORDA are an important consideration.

Resilience threats can be roughly characterized into natural threats, man-made threats, and accidents. ORDA focuses on the man-made threat of targeted disinformation that is used to impact an organization's ability to make decisions. This disinformation is propagated primarily through data and analytics being used by the organizations and can be introduced by an outsider to the organization, or by a malicious insider. For this analysis, we define disinformation campaigns as activities that are intended to cause harm; these are distinguished from misinformation, which is false information that may be unintentionally spread [7]. For the purpose of this scoping exercise, we are only considering disinformation attacks initiated by outsiders to the organization (i.e., insider threats are not included within this scope).

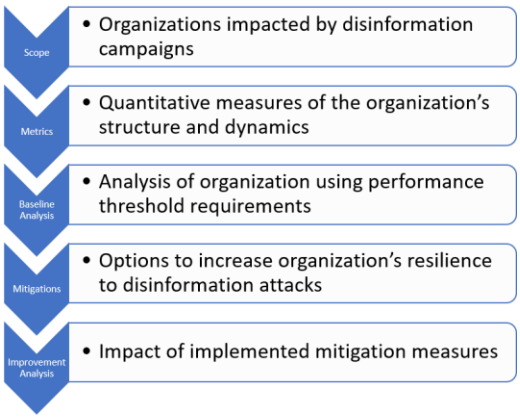

Fig. 1. Steps in the ORDA Framework.

The resilience goals of an analysis should address the primary stages of preparing for, withstanding, and recovering from a given threat. In this case, the "prepare" stage consists of the period of time before the organization has to make a consequential decision using the data/analytics that have impacted by disinformation. The goal here would be to potentially identify the presence of disinformation in the datasets or analyses before a decision is made with that data. The organization could develop redundant data streams to help with detection, or alternatively reduce the influence of any single data source on overall decision-making. During the "withstand" phase, in which a disinformation attack is already underway, the goal is for the organization to be able to adapt by using alternative datasets to make decisions, and to have measures in place to monitor and identify ongoing disinformation attacks. Lastly, during the "recover" phase, the organization will need to overcome the effects of a disinformation attack. Since we are specifically looking at decision-making organizations, the goal during this phase is for the organization to have confidence in the data and processes being used and continue to be able to make impactful decisions. A summary of this first step for ORDA is given in Table I.

B. Metrics

The second step of the ORDA framework defines the metrics that will be used in the analysis. For this step, the goal is to move from the qualitative organizational resilience metrics described in Section II to quantitative metrics that capture organizational dynamics. Quantitative metrics will allow the team to measure baseline resilience to disinformation within organizations and to measure improvements once mitigation measures have been implemented (Fig. 1).

For each organizational attribute found in organizational resilience research, the team evaluated whether the attribute applied to disinformation attacks, whether it was relevant, and what types of quantitative metrics could be used to represent the attribute. This down selected set of attributes and their corresponding quantitative metrics are described in Table II.

These are proposed metrics for the ORDA framework. However, further research is needed to determine whether these metrics are actually indicative of an organization's resilience to disinformation attacks (vs. a general characteristic that does not need to be included in ORDA). Furthermore, the metrics available for implementation may depend on the data availability of different organizations.

TABLE I. Scope and Goals

Category	Scope
System	Decision-making organizations
Threats	Man-made disinformation attacks propogated through data/analytics by entities outside of the organization
Resilience Goals	Prepare: Develop redundant data streams to counter disinformation-compromised datasets; introduce safeguards to detect disinformation in datasets Withstand: Use alternative datasets, monitor and identify ongoing disinformation attacks Recover: Have confidence in data being used to make decisions

TABLE II. METRICS

Organizational Attribute	Quantitative Metrics
Situational Monitoring & Reporting	• Data monitoring—frequency, quality, source verification • Level of redundancy in datasets to verify information • Number of external influences on organizational priorities
Managing Vulnerabilities/ Anticipating Events and Threats	• Verification of data through further experiments (binary or time) • Air gapped redundant networks (binary or number) • Similarity of datasets used for decision making • Number of backup/alternate data sources
Having Resources	• Number of servers, analysts, and decision makers as percentage of how many are needed
Innovation/ Creativity	• Percentage of revenue/budget/work hours dedicated to training, new analysis methods, research, etc.
Organizational Transparency	• Number of groups/functions contributing to the decision process • Number of levels of decision making • Number of decision makers per organizational level • Number of feedback loops during decision making process (checks)
Margin/Workload	• Number of projects/priorities • Percentage allocated (analysts, decision makers, etc.) • Number hours worked/projected hours • Number hours to make decision (or time limit binary)
Locations of the Organization	• Number of locations • Rate of disinformation attacks in each area • Which facilities have decision makers and number

C. Baseline Analysis

The baseline analysis step within the ORDA framework is perhaps the point of greatest deviation from a traditional energy and infrastructure resilience analysis. For the latter, we assess the system(s) of interest during normal operations, when they are not experiencing threats, to evaluate baselines. However, it may not be possible for an organization to know whether they are experiencing a disinformation attack. The organization could appear to be in steady state while already bringing in data that has been altered with disinformation. In the context of decision-making organizations, we propose that the ultimate goal of an organization is to be able to make impactful decisions within a reasonable timeframe that have a desired effectiveness. Therefore, rather than comparing performance during a non-event period, this research will use performance threshold requirements (derived from Quantifications of Margins and Uncertainties [8]) as the model baseline for ORDA.

There are multiple considerations in assessing the organization's baseline in this manner. First, the threat space will need to be represented as part of the assessment inputs and design. Researchers will need to understand the different injection points for disinformation attacks against organizations and how those vary based on whether the attacker is an outsider or an insider. The injection points will also determine what parts of the organization are being impacted by the disinformation attack(s). For example, an injection point that occurs at the point where data is being transferred to the organization may impact a single dataset, while an injection point between analysis being done using a dataset and the transfer of those findings to decision makers could have an internal impact that bypasses safeguards that only check the datasets upon initial receipt.

Another consideration is that researchers will need to have a functional decomposition of groups within the organization to understand the specific roles and activities of each. Examples of functional groups within an organization would be entities such as analysts, leadership, human resources, etc. These would then be mapped to functions they perform such as data gathering, decision making, etc.; this may not be a one-to-one mapping (see additional details in the following section). Similarly, researchers need to have a functional decomposition of data types used by the organization to the missions they enable/impact. This will be particularly important when understanding how an organization can use alternate datasets or tracing the impacts of a disinformation attack on a specific dataset/analysis.

D. Mitigations

The fourth step of the ORDA framework considers mitigation options to increase an organization's resilience to disinformation attacks. At a high level though, the mitigation measures address the following questions:

- Which metrics have a quantifiably significant effect on organization resilience?
- Are these consistent across different organizations?
- Do metrics scale linearly or non-linearly (across time and/or events) for intended outcomes, or are there diminishing returns after a certain level?
- Are there metrics that are negatively correlated?
- Are there any metrics that are interchangeable?
- Are there any metrics whose impact on resilience is negligible?

Here the term metrics is referring to the quantitative metrics identified in Table II. The goal of this research is to understand which metrics have a statistically significant impact on an organization's ability to prepare for, withstand, and recover from disinformation attacks. Different metrics may have a greater impact on one of these phases of resilience than another, which we will be aiming to understand in more detail. Additionally, some metrics may be interchangeable, which would give organizations flexibility in which areas to target when trying to improve resilience.

Various research questions are present in this area, including whether the levers to improve resilience are consistent across different types and sizes of organizations or whether these levers are specific to a given organization. This learning alone will provide powerful insight as to how organizations can better insulate themselves from the impacts of disinformation attacks in the future. Additional details about how modeling can be leveraged to help answer these questions are listed in Section IV.

E. Improvement Analysis

The final step of the ORDA framework is to measure the impact of mitigation measures once they have been implemented in the real-world for an organization. This is beyond the scope of this initial research, but in general, refers to the iterative process needed to ensure assessments are being used to support real-world decisions. For example, if real-world performance differs from the performance forecasted by the models, we will restart the resilience analysis process. Alternatively, this analysis can be done as a benchtop exercise by looking at how mitigation measures implemented in the models perform when the threat vector is changed. These exercises can give insight into the robustness of proposed measures and their ability to transfer across different disinformation attack scenarios.

IV. Modeling Organizational Resilience

Various modeling approaches have been used to simulate organizational behaviors, including agent-based models, system dynamics models, and cellular automata models [9]. Another approach called viable systems modeling (VSM) has also been used to represent organizations by defining the organizational structure, dependencies between various subsystems within the organization, command and control channels between the subsystems, and the flow of data and information [10]. The VSM focuses on five subsystems, that are generally described for flexibility and not specific to the decision-making organizations. However, the representation of key functional and informational flow concepts defined within VSM may be particularly well-suited to represent decision-making organizations that are subject to disinformation attacks. Therefore, an initial exercise was undertaken to map the quantitative organizational resilience metrics and decision-making processes to the areas of the VSM that they will impact. These mappings are captured in Table III. For simplicity, the five VSM subsystems are defined based on their organizational role in decision making.

Each subsystem, as mentioned, provides command and control, as well as support, to the operational units via one of a series of channels. For example, the resources required for the operational unit to function are defined and provided via a resource channel from the resource unit. An auditing channel reviews the operational unit's processes to ensure resources are used adequately, and if the operational unit requires additional resources, this is requested and negotiated, and then provided from the resource unit via the channels. As such, the operational unit and the resource unit handle resource management, margin, and workload balancing of the subsystem conducting the analysis. The unit that conducts the environmental monitoring for the system is the situational awareness unit which, for our organizational definition, also supports scanning for relevant external datasets for the use by the operational unit. As such, the situational awareness & data collection unit is responsible for detection and sharing of external issues (e.g., events, threats, and opportunities) and relevant data (e.g., collected or provided from external systems) to the analysis unit and/or the decision-making unit (both operational units) via the environmental scanning channel. In Fig. 2, a simplified organizational system is mapped using the VSM. We have included both operational units—the analysis unit and the decision-making unit (presented in blue). The dotted green line between reflects the movement of datasets or analysis products between the units. The figure also highlights, in grey, the other four subsystems and their respective command and control channels.

TABLE III. VSM Subsystems Mapped to Metrics

VSM Subsystem	Relevant Organizational Attribute	Purpose/Function
Operational Unit	• Resource Management • Margin/Workload • Situational Monitoring & Reporting • Managing Vulnerabilities	Supports the process of data analysis (analysis unit) or the process of decision making (decision-making unit)
Coordination Unit	• Organizational Transparency	Responsible for coordination and control between operational units. May include use of standards or formalized requirements.
Resource Unit	• Resource Management • Margin/Workload	Maintains the operations of the individual operational units within the system and is responsible for resource allocation
Situational Awareness & Data Collection Unit	• Situational Monitoring & Reporting • Managing Vulnerabilities • Anticipating Events and Threats • Innovation/Creativity	Scans environment and communicates issues and opportunities as well as collects external data for use in analysis
System Policy & Identity	• Locations of Organization • Innovation/Creativity	Defines system's organizational objectives, balances intersts of the system, and ensures focus

Fig. 2 also captures two example disinformation scenarios we consider within the context of the VSM (shown as lines from the attacker to the organization system). The first scenario is an attack targeting external datasets prior to their entry into the organization. In this scenario the resilience metrics would be focused on the processes within the situational awareness & data collection units to prevent ingestion of the disinformation, as well as on the analysis unit to ensure the disinformation is not processed as part of its analysis. The supporting subsystems, resources, system policy, and coordination, all support the resilience of both the analysis unit and the situational awareness & data collection unit to the disinformation attack. The second scenario is an attack on the analysis product affecting the decision-making ability of the system to 'trust' its own analysis. In this situation, not only does the analysis unit require support from all the subsystems, but the decision-making unit would also require support from the situational awareness unit specifically to help them recognize the attack.

Although the VSM approach provides a powerful qualitative platform for understanding organizational functions and interactions, the actual assessment of organizational behaviors requires the ability to simulate different outcomes. Thus, alternate modeling approaches, such as multi-player, agent-based models (ABM), will be important to support study of

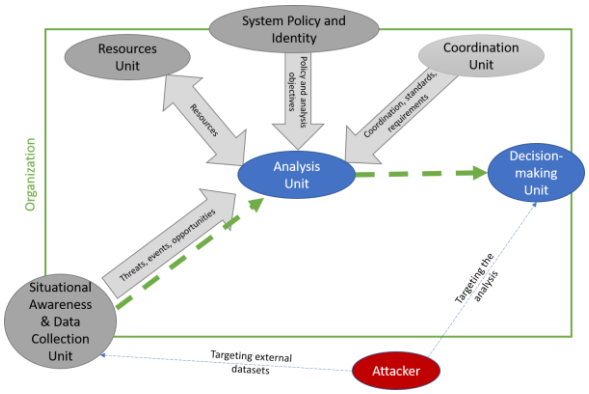

Fig. 2. Simplified Organizational Representation Highlighting Two Possible Disinformation Attacks.

exemplar organizations that have experienced disinformation attacks. Outcomes from these ABMs can inform which quantitative metrics have the largest influence on organizational resilience to disinformation and support assessment of metric transferability across different organizations.

V. Evaluating Organizational Resilience

So far, we have discussed ways to model organizations and possible metrics that can help quantify various aspects of an organization that we believe to influence resilience to disinformation attacks. However, we still need a way to assess the overall resilience of a given organization after working through the steps of the ORDA framework. Traditional assessments in organizational resilience research have focused on organization outcomes such as change in profit, income, product cost, manpower, etc.; or on recovery-based measures such as recovery time, potential loss averted, ratio of recovery and loss, total loss over time, etc. [5], [11]. While these are useful ways to assess resilience in organizations that are experiencing more historically typical disruptions in supply chains, operating hours, etc., they do not capture the novel consequences posed by disinformation attacks.

Since we are focusing on organizations who are using data/analytics to make high-consequence decisions, the ultimate measure of how resilient an organization is to disinformation attacks will consist of two important components—whether an organization can make a decision within a desired timeframe, and the ability of that decision to have a "positive" outcome as defined by the organization's mission(s) or objectives(s). The organization will need to demonstrate these two components of resilience across decisions being made to be considered resilient to disinformation attacks.

We posit that the barriers to an organization being able to make these high-quality decisions in a timely manner can be effectively quantified through a "decision impedance" metric. The goal of adversaries launching a disinformation attack against the organization will be to increase decision impedance, while the goal of the organization will be to put mitigation efforts into place to increase resilience and lower decision impedance. We represent decision impedance as:

$$I_D = T_D/Q_D, \text{ where} \quad (1)$$

I_D is the decision impedance associated with decision D, T_D is the time it took for the organization to make decision D, and Q_D is the quality of decision D.

The specific units for these variables will require future research. For example, T_D could be represented in hours or as a ratio of actual hours to desired hours and representing Q_D as the amount of time without negative consequences as a result of the decision. Q_D would likely need to have an upper limit based on the goals of the organization. Long-range simulation and subsequent data collection would be needed to assess the accuracy of these results with respect to organizational characteristics (e.g., cost and consequence).

All mitigation measures put in place by organizations to increase resilience to disinformation attacks will have a corresponding cost to the organization. Because budgets are rarely unlimited, there will be different mitigation measures available to the organization at different price points [12]. Another goal of this research is to determine the optimal mitigation measures at a set investment cost to minimize decision impedance to the organization. The tradeoff between cost and decision impedance will likely result in a Pareto frontier (see Fig. 3 for an example) of potential mitigation measure options that organizations may choose from when deciding how to increase resilience.

The top-left most option (shown in orange) specifies what will happen if an organization makes no investments in mitigation measures to increase organizational resilience to disinformation attacks. The associated cost is zero, but decision impedance is at a maximum, meaning that it takes the organization longer than desired to make a decision and/or that the quality of that decision is below an acceptable threshold; this threshold could be unique to a given organization and is represented by the green line in Fig. 3. Research is needed to determine acceptable thresholds.

The bottom-right most option (shown in blue) specifies the opposite extreme—decision impedance has been reduced as much as possible through implemented mitigation measures, but those measures are associated with a maximum cost. While this would be best-case from the perspective of being able to make decisions, most organizations' budgets will not allow for this level of investment and such lavish outlay of capital could have other negative impacts on the organization.

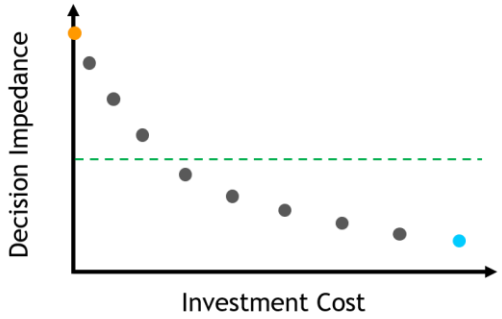

Fig. 3. Example Pareto Frontier of Cost vs. Decision Impedance.

Though each of the hypothetical options shown in Fig. 3 is Pareto optimal, the most practical options tend to lay at the elbow of the curve where decision impedance has been lowered, but solutions are still affordable to the organization. The determination of what mitigation options make sense and are affordable is usually solicited through conversations with organizational decision-makers. These discussions provide insights into organization priorities, and acceptable risk levels to the organization based on the nature of the decisions they are making with data that may be subject to disinformation attacks.

VI. Discussion

The threat disinformation poses to organizations who need to make high-consequence decisions based on data and analytics is rapidly evolving and novel approaches are needed near-term. The expansion of threat-informed resilience analysis and resilience frameworks traditionally used for energy and infrastructure into the ORDA framework offers one avenue to begin tackling this problem. By determining which attributes help increase organization resilience to disinformation attacks, researchers can help protect critical organizations that work on behalf of national security, public safety, and other missions.

There are a number of research needs related to ORDA that require further attention. For example, given that organizations are constantly in flux, quantitative metrics will need to consider both topological (i.e., structural) and dynamic properties of an organization's behavior. Topological metrics could capture organizational characteristics around decision-making structure while dynamic metrics will consider the evolution of the system over time to effectively capture the consequences as well as responses needed to improve resilience. As noted in Section II, the impact of disinformation attacks within organizations depends heavily on both system and human characteristics, thus metrics will be needed to effectively capture the interactions of these components. Although some mathematical equations to support quantification of these complex relationships exist – e.g., co-occurrence vs similarity [13] and feedback density [14] – numerous questions still persist regarding effective implementation of these metrics to support overall resilience objectives. For example, how should geographic disparities be captured in quantitative assessments, and how do we balance competing objectives driving organizational behaviors to ultimately support resilience? Some of these answers could be explored through the development of ABMs as noted above. In general, ongoing research is needed to elucidate answers to these complex ORDA questions.

Acknowledgment

The authors would like to thank Steve Verzi for feedback on an earlier version of this manuscript. This work is funded by the Laboratory Directed Research and Development program at Sandia National Laboratories. Sandia is a multimission laboratory managed and operated by National Technology and Engineering. Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525. The views expressed in the article do not necessarily represent the views of the U.S. Department of Energy or the United States Government. SAND2022-7133 C.

References

[1] E. D. Vugrin, D. E. Warren, M. A. Ehlen and R. C. Camphouse, "A Framework for Assessing the Resilience of Infrastructure and Economic Systems," in *Sustainable and Resilient Critical Infrastructure Systems*, Berlin, Springer, 2010, pp. 77-116.

[2] PPD-21, "Presidential Policy Directive 21: Critical Infrastructure Security and Resilience," Executive Office of the President, Washington D.C., 2013.

[3] K. Shu, A. Bhattacharjee, F. Alatawi, T. Nazer, K. Ding, M. Karami and H. Liu, "Combating disinformation in a social media age," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery,* vol. 10, no. 6, p. e1385, 2020.

[4] S. T. Smith, E. K. Kao, E. D. Mackin, D. C. Shah, O. Simek and D. B. Rubin, "Automatic detection of influential actors in disinformation networks," *Proceedings of the National Academy of Sciences,* vol. 118, no. 4, 2021.

[5] C. Ruiz-Martin, A. López-Paredes and G. Wainer, "What we know and do not know about organizational resilience," *International Journal of Production Management and Engineering,* vol. 6, no. 1, pp. 11-28, 2018.

[6] A. Wachtel, K. A. Jones, M. J. Baca, E. O'Neill-Carrillo and M. B. DeMenno, "Resilient Energy Systems Strategic Initiative: Sandia's Integrated Methodology for Energy and Infrastructure Resilience Analysis," Sandia National Laboratories, Albuquerque, 2020.

[7] J. H. Fetzer, "Disinormation: The use of false information," *Minds and Machines,* vol. 14, no. 2, pp. 231-240, 2004.

[8] M. Pilch, T. G. Trucano and J. C. Helton, "Ideas Underlying Quantification of Margins and Uncertainties (QMU): A White Paper," Sandia National Laboratories, Albuquerque, 2006.

[9] J. R. Harrison, Z. Lin, G. R. Carroll and K. M. Carley, "Simulation modeling in organizational and management research," *Academy of management review,* vol. 32, no. 4, pp. 1229-1245, 2007.

[10] B. Williams and R. Hammelbrunner, Systems Concepts in Action: A Practitioner's Toolkit, California: Stanford University Press, 2010.

[11] M. Baghersad and C. W. Zobel, "Organizational Resilience to Disruption Risks: Developing Metrics and Testing Effectiveness of Operational Strategies," *Risk Analysis,* vol. 0, no. 0, 2021.

[12] Z. Lin and K. M. Carley, "Organizational reponse: The cost performance tradeoff," *Management Science,* vol. 43, no. 2, pp. 217-234, 1997.

[13] K. P. Mainali, E. Slud, M. C. Singer and W. F. Fagan, "A better index for analysis of co-occurrence and similarity," *Science Advances,* vol. 8, no. 4, p. eabj9204, 2022.

[14] A. Naugle, S. Verzi, K. Lakkaraju, L. Swiler, C. Warrender, M. Bernard and V. Romero, "Feedback density and causal complexity of simulation model structure," *Journal of Simulation,* pp. 1-11, 2021.