SAND2022-12450C

Sandia National Laboratories

Application of Resilience Theory to Organizations Subject to Disinformation Campaigns

Amanda Wachtel*, Susan Caskey, Thushara Gunda, Elizabeth Kistin Keller, and Olga Hart
Sandia National Laboratories, *Contact: awachte@sandia.gov

Problem

Community, corporate, and government organizations are being targeted by disinformation attacks at an unprecedented rate [1]. These attacks:

- Interrupt the ability of organizations to make high-consequence decisions
- Target multiple areas within the organization
- Lower organizational confidence in datasets and analytics

Fig. 1. Injection points for disinformation within organizations can span across data, analytics, and decision-making.

Expansion of resilience theory applications to disinformation are needed to advance research that: 1) determines relevant metrics and 2) identifies mitigations needed to increase organizational resilience to disinformation.

Related Literature

This work brings together three fields of research:

- Evaluation of disinformation impacts [2]
- Organizational resilience [3]
- Infrastructure resilience [4]

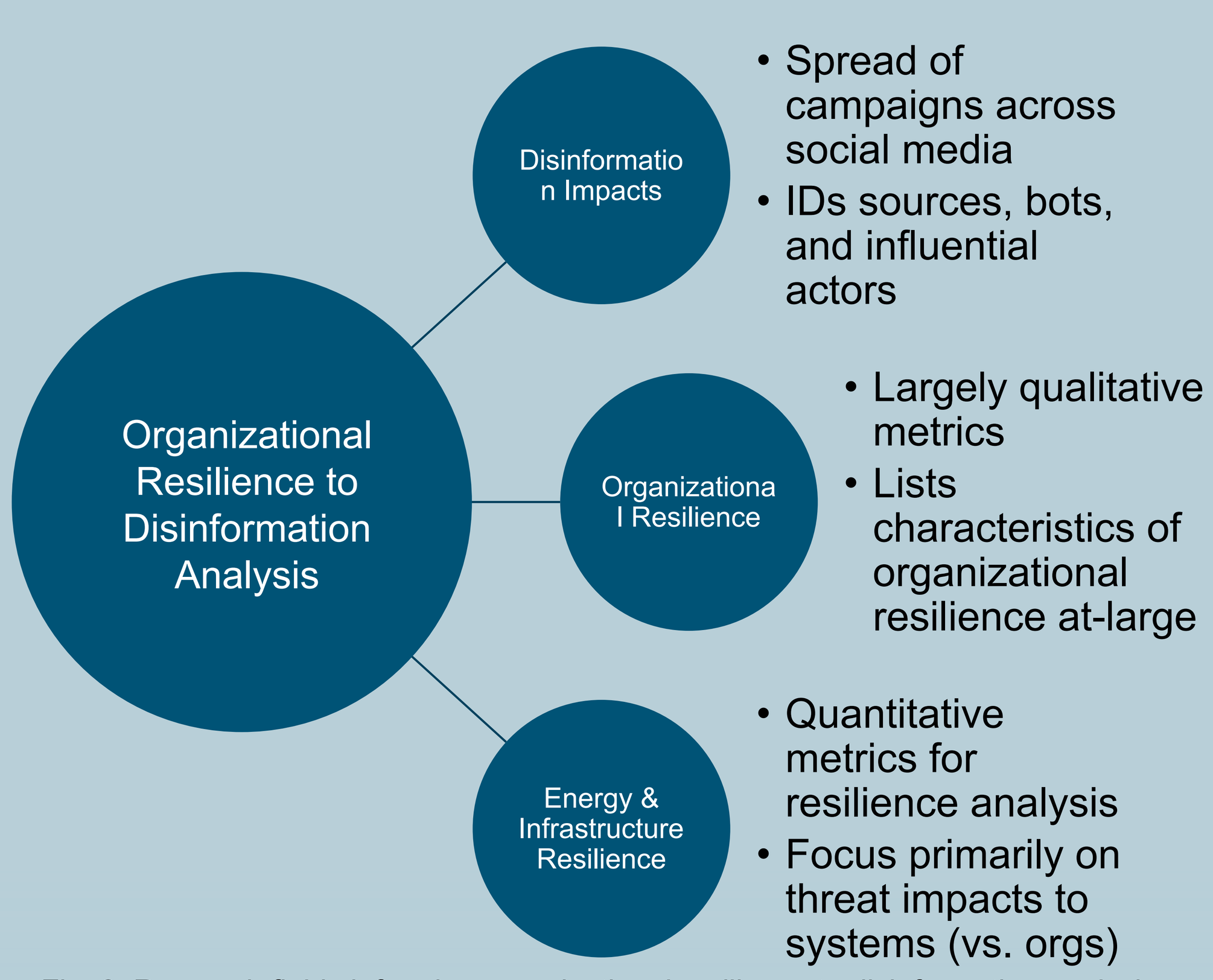

Fig. 2. Research fields informing organizational resilience to disinformation analysis.

Each field brings elements needed for organizational resilience to disinformation analysis (ORDA) but none address all aspects. ORDA requires understanding of how disinformation spreads through organizations (including the human element) as well as development of quantitative metrics customized for organizational resilience.

Scope & Metrics

This work adapts Sandia's Integrated Methodology for Energy and Infrastructure Resilience Analysis – a threat-informed, consequence-focused, and performance-based approach [4] – to support the ORDA framework.

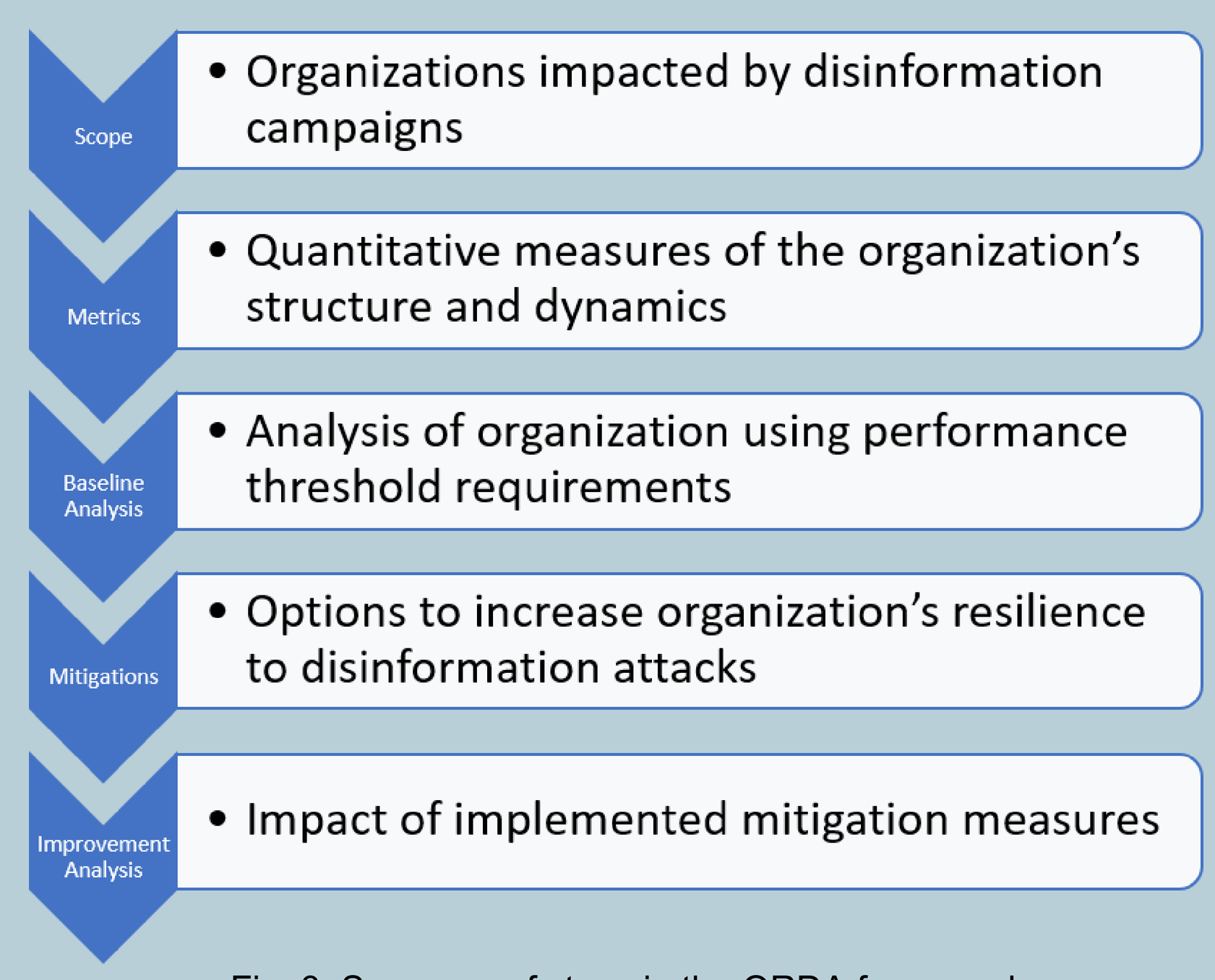

Fig. 3. Summary of steps in the ORDA framework.

Scope: We focus specifically on organizations who use data to make high-consequence decisions. Organizations can exhibit resilience to disinformation before, during, or after an attack.

TABLE I. Scope and goals of ORDA

Category	Scope
System	Decision-making organizations
Threats	Man-made disinformation attacks propagated 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

Metrics: For each organizational attribute found in organizational resilience research, the team evaluated whether it applied to disinformation attacks, how it was relevant, and the types of quantitative metrics that could be used to represent the attribute.

TABLE II. ORDA Metrics

Organizational Attribute	Quantitative Metrics
Situational Monitoring & Reporting	1. Data monitoring—frequency, quality, source verification 2. Level of redundancy in datasets to verify information 3. Number of external influences on organizational priorities
Managing Vulnerabilities/ Anticipating Events and Threats	1. Verification of data through further experiments (binary or time) 2. Air gapped redundant networks (binary or number) 3. Similarity of datasets used for decision making 4. Number of backup/alternate data sources
Having Resources	1. Number of servers, analysts, and decision makers as percentage of how many are needed
Innovation/ Creativity	1. Percentage of revenue/budget/work hours dedicated to training, new analysis methods, research, etc.
Organizational Transparency	1. Number of groups/functions contributing to the decision process 2. Number of levels of decision making 3. Number of decision makers per organizational level 4. Number of feedback loops during decision making process (checks)
Margin/Workload	1. Number of projects/priorities 2. Percentage allocated (analysts, decision makers, etc.) 3. Number hours worked/projected hours 4. Number hours to make decision (or time limit binary)
Locations of the Organization	1. Number of locations 2. Rate of disinformation attacks in each area 3. Which facilities have decision makers and number

Furt[illegible] whic[illegible] organization's resilience vs. which are general characteristics. Metrics also depend on data availability.

Modeling and Simulation

Viable systems modeling (VSM) is used to represent organizational structure, with five subsystems used to represent key functions and the flow of information [5].

TABLE III. VSM Subsystems mapped to ORDA metrics

VSM Subsystem	Relevant Organizational Attribute	Purpose/Function
Operational Unit	1. Resource Management 2. Margin/Workload 3. Situational Monitoring & Reporting 4. Managing Vulnerabilities	Supports the process of data analysis (analysis unit) or the process of decision making (decision-making unit)
Coordination Unit	1. Organizational Transparency	Responsible for coordination and control between operational units. May include use of standards or formalized requirements.
Resource Unit	1. Resource Management 2. Margin/Workload	Maintains the operations of the individual operational units within the system and is responsible for resource allocation
Situational Awareness & Data Collection Unit	1. Situational Monitoring & Reporting 2. Managing Vulnerabilities 3. Anticipating Events and Threats 4. Innovation/Creativity	Scans environment and communicates issues and opportunities as well as collects external data for use in analysis
System Policy & Identity	1. Locations of Organization 2. Innovation/Creativity	Defines system's organizational objectives, balances interests of the system, and ensures focus

A VSM mapping of a simple organization can show different types of units (data collection, analysis, and decision-making) as well as the flow of information between units across sc

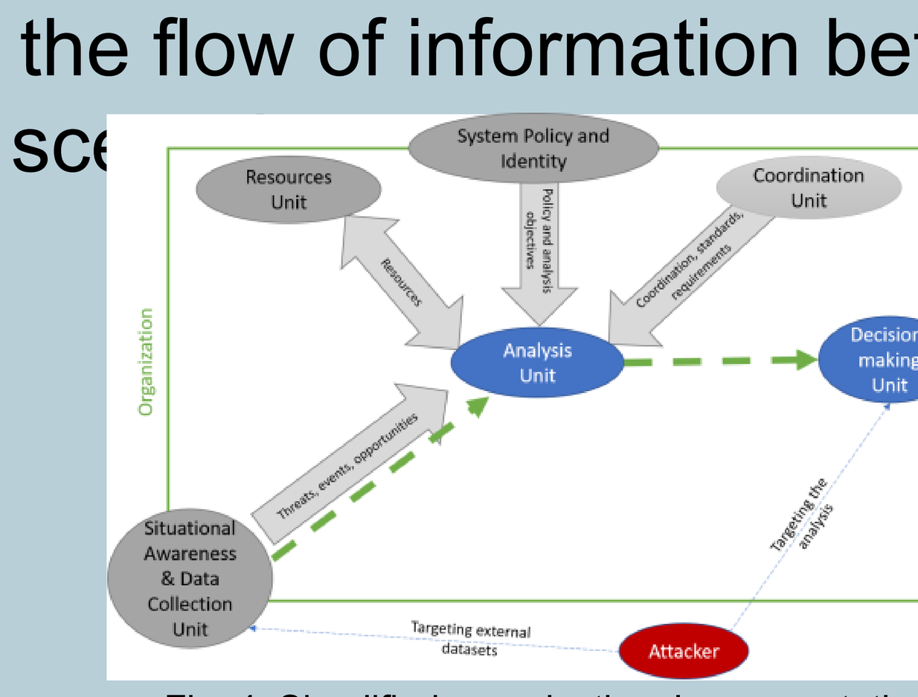

Fig. 4. Simplified organizational representation highlighting two possible disinformation attacks.

Further research is needed to combine VSM logic with quantitative modeling approaches to support metrics and mitigation

Resilience Evaluations

Resilience to disinformation attacks will consist of two components: 1) whether an organization can make a decision within a desired timeframe and 2) the ability of that decision to have a "positive" outcome. We strive to minimize *decision impedance* — the time it takes to make decision D, over the quality of decision D. $I_D = T_D/Q_D$

The tradeoff between cost and decision impedance will likely result in a Pareto frontier. Research is needed to determine appropri[illegible] below).

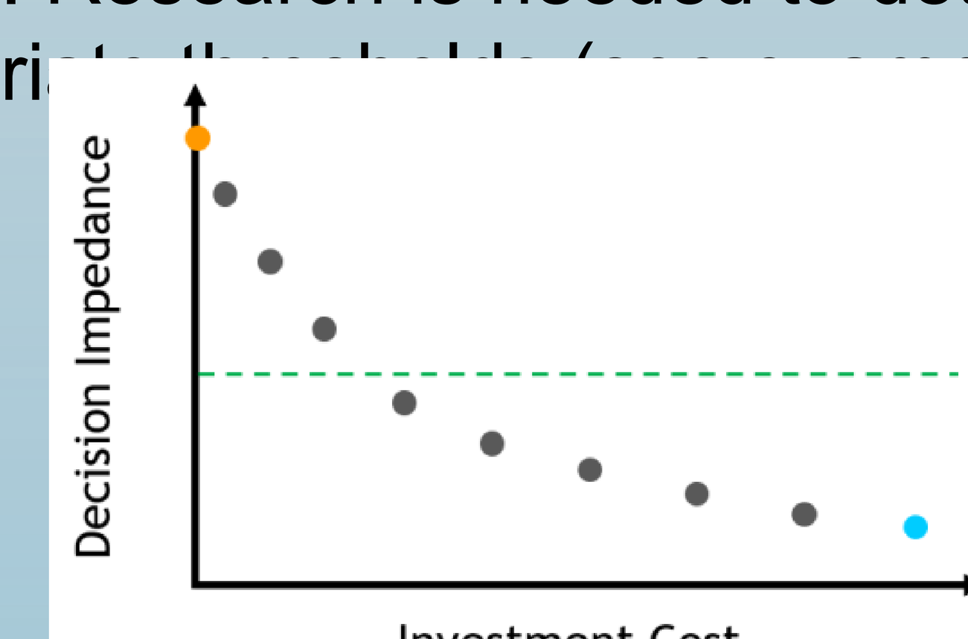

Fig. 5. Example Pareto frontier of cost vs. decision impedance. Green line indicates example threshold.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & 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-NA0003525.
SAND No. ___________

References
[1] L. Rodriguez-Fernandez. Disinformation and organisational communication: A study of the impact of fake news. Technical report, Revista Latina de Comunicacion Social, November 2019.
[2] K. Shu et al., "Combating disinformation in a social media age," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 2020.
[3] C. Ruiz-Martin et al., "What we know and do not know about organizational resilience," *International Journal of Production Management and Engineering*, 2018.
[4] A. Wachtel et al., "Resilient Energy Systems Strategic Initiative: Sandia's Integrated Methodology for Energy and Infrastructure Resilience Analysis," Sandia National Laboratories, Albuquerque, 2020.
[5] B. Williams and R. Hammelbrunner, *Systems Concepts in Action: A Practitioner's Toolkit,* California: Stanford University Press, 2010.

Additional details about this work are captured in associated paper that will be published as part of the Resilience Week 2022 Proceedings.

LABORATORY DIRECTED RESEARCH & DEVELOPMENT

Sandia National Laboratories