SAND2023-08838J

33rd Annual INCOSE international symposium
hybrid event
Honolulu, HI, USA
July 15 - 20, 2023

Organizational System Resilience to Disinformation: A Viable Systems Model Exploration

Susan Caskey
Sandia National Laboratories
PO Box 5800 M/S 1373
Albuquerque, NM 87185
505-284-5095
sacaske@sandia.gov

Thushara Gunda
Sandia National Laboratories
PO Box 5800 M/S 1137
Albuquerque, NM 87185
505-845-3440
tgunda@sandia.gov

Abstract. This paper explores the utility of organizational system modeling frameworks to provide valuable insight into information flows within organizations and subsequently, opportunities for resilience against disinformation campaigns targeting the system's ability to utilize information within its decision making. Disinformation is a growing challenge for many organizations and in recent years has created delay in decision making. The paper has utilized the viable systems model (VSM) to characterize organizational systems and used this to outline potential subsystem requirements to promote resilience of the system. The results of this paper can support the development of simulations and models considering the human elements within the system as well as support the development of quantitative measures of resilience.

Introduction

Disinformation is defined in the scope of this paper as active campaigns of false information, which has the intent to create negative impact. Disinformation campaigns are a malicious act targeting information used in decision making by organizations (or even an individual) with the objective to impede the decisions or actions resulting from the decision (Rodríguez-Fernández, 2019).

Disinformation is not a new concept, as examples of altered information used to control the actions of a population have been documented as far back at the 16th century (Socialtrendly INC, 2021). It is suspected that disinformation campaigns originate even far earlier in human history. However, with the explosion of information and information sources broadly accessible by the public, coupled with the ease at which information can be altered, we are witnessing new opportunities for those with malicious intent to misuse information.

For organizations, such as those tasked with making governmental-level decisions, the risks associated with delay or inaccuracy in decision making can be significant. Consider the Office of the Prohibition of Chemical Weapons (OPCW), an international organization tasked with oversight of chemical weapons. Media reporting indicates that disinformation campaigns negatively impacted the OPCW's ability to monitor and respond to the use of chemical weapons by the Syrian government in 2017 (United Nations, 2021).

Understanding how information moves into, within, and outside the system can inform the resilience – i.e., the ability to withstand, absorb, and quickly recover from (Rodríguez-Fernández, 2019).– of an organizational system to disinformation. Such insights, subsequently, could also help the organization implement appropriate governance to enhance their resiliency. The purpose of this paper is to explore the utility of organizational system modeling frameworks for providing insight into information flows within organizations and subsequently, opportunities for resilience. The first section will outline the organizational system modeling utilized in this paper; this will be followed by the application of the modeling framework on two relevant case studies. Our paper concludes with a discussion reflecting on the requirements of system elements (i.e., subsystems) to support overall system resilience to disinformation.

Organizational System Modeling

There are multiple approaches for modeling organizations (Ashworth & Carley, 2007). One such approach is a viable systems model (VSM), whose specific aim is to characterize the system's ability to remain viable (e.g., has the ability to maintain performance) the event of various system and environmental perturbations (Williams & Hammelbrunner, 2010). In essence, viability is the ability of a system to maintain a separate existence. VSM was introduced in the 1970s by Stanford Beer and is widely recognized by Beer's implementation of the model on Chile's economy system (Perez, 2012). In the VSM, an organizational system is defined based on performance of a set of 5 subsystems, spanning operations to coordination and policy (Table 1). The VSM has been used to consider multiple attributes of organization systems, specifically the communication and information flow (Kirikova & Pudane, 2013), (Rezaee, Azar, Ba Erz, & Nayeri, 2019), (Keating C. , 2000). As such, we have decided a VSM is particularly well-suited to represent organizations that are subject to disinformation attacks.

In addition to the functions, a VSM includes a series of channels that support communication between the subsystems. These include the Command Channel, the Resource bargain and accountability channel, the Operations channel, the Coordination channel, the Environmental Scanning Channel, and the Algedonic Channel.

In this study, we are defining our organizational system as a system who uses information to support decision making. In this implementation, the operational unit (S1) of focus has been defined as the process that takes inputted data, transfers this data into information using processing and analytics (data analysis) and then presents this information (the S1 output) for use in knowledgeable decision making (Figure 1).

Table 1. VSM Subsystems

Subsystem (VSM Label)	**Purpose**
Operational Unit (S1)	This is the operational or implementation subsystem that performs tasks directly in support of the overall system objective.
Coordination (S2)	Communicates standards / procedures to the Operation Unit (S1s) and aligns schedules and tasking between each S1. Prevents unnecessary oscillation and conflict within the system.

System Operations (S3) & Audit (S3*)	Maintains the operations of the individual operational units, S1s, within the system and is also responsible for resource allocation and performance accountability.
	*Ensures operations of each S1 and between the S1 are performing within established expectations. Examines anomalies in performance.
System Development (S4)	Scans the environment considering future threats or opportunities – specifically promotes situational awareness and opportunities for innovation. This subsystem also pulls data from the environment for use by the operational unit.
Policy and Identity (S5)	Defines the system's organizational objectives, balances interests of the system, and ensures focus for consistency in decisions, actions, and interpretations.

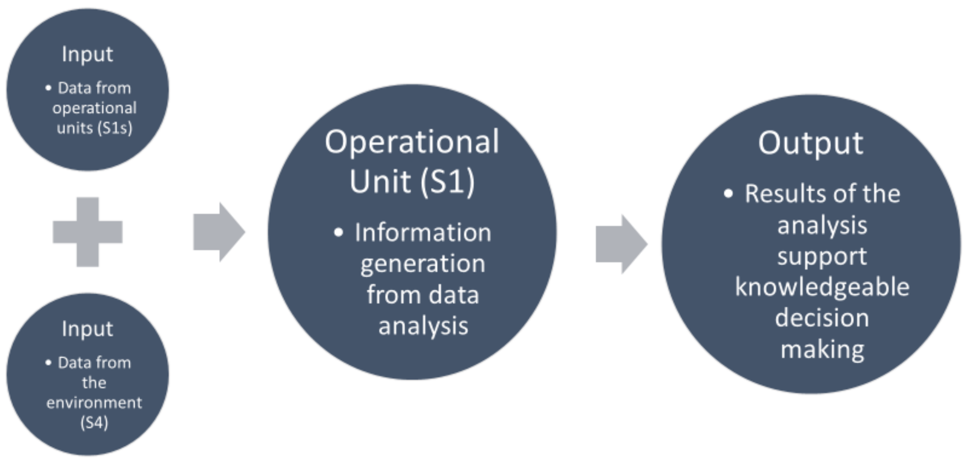

Figure 1. Input to output reflected as the function of the operational unit. Input or data is provided to the operational unit from both the system development subsystem as well as the other operational units within the organization. This data is then used in the analysis, which is then provided as the output of our subsystem to the decision maker.

The team specifically outlined governance and influences on the operational unit (S1) by the other subsystems that support information analysis process and enhance resilience to disinformation. These include:

- The Policy and Identify (S5) defines the analysis objective of the operational unit (what is the knowledge needed) based on the organizational policies/mandates.
- Coordination (S2) ensures outputs from other operational units are available as inputs with sufficient metadata to support to allow verification and validation of the data as well as provide ability for thoughtful consideration of the data prior to use (i.e., confidence management) by the S1. This subsystem also supports robustness of the input of data from external systems (the S4).
- The System Operations & Audit (S3 & S3*) support ensuring resources including people, tools, logistics, etc. are available and sufficient to the operational unit to support the data analysis requirements to include confidence management.

- System Development (S4) ensures both opportunities - such as new data or new analysis processes (innovation) - are considered and supports understanding potential issues or threats (situational awareness) to the analysis process from outside the system (e.g., the environment).

Implementation of the VSM, based on the defined role of the operational unit, can provide valuable insight into understanding possible vulnerabilities and opportunities for improving organizational resilience in the presence of disinformation. The remainder of this paper focuses on using case studies to understand key mechanisms and potential gaps that could impact a system's resilience to disinformation.

Case Studies

Two case studies were used to evaluate the utility of the VSM-informed information flow model for evaluations of disinformation impact for organizations. The first relates to OPCW, focusing on their role in the determination of who conducted the chemical weapons attacks detected in Syria in 2017 (United Nations, 2020) while the second focuses on the Global Polio Eradication Initiative (GPEI) in Nigeria (Jegede, 2007). Both organizations were impacted by disinformation attacks and as such, offered the team relevant examples to consider the organizational structure in the presence of disinformation attacks.

The following subsection dives into these two case studies by first providing background and context descriptions before applying the VSM. Then system gaps (identified through the framing as a VSM) that impacted the system's resilience to disinformation campaigns are then summarized.

OPCW

Background: OPCW's mission is to support compliance with the Chemical Weapons Convention (CWC), while promoting chemical industrial development. Under this mission, OPCW – in partnership with the United Nations (UN) – initiated an investigation into the alleged use of chemical weapons within Syria following Syria's ratification of the CWC in 2013. In 2014, a joint fact-finding mission was set up to confirm use of a chemical weapon as defined by the CWC in Syria (OPCW, 2021). Following the confirmed use, a joint investigative mechanism between OPCW and the UN was established to determine the perpetrators of the use. This joint investigative mechanism was not renewed in 2017. However, as there were confirmed chemical weapons used in Syria following the dissolving of the joint investigative mechanism, OPCW established their own investigation and identification team (IIT) (OPCW, 2021).

The IIT conducted a detailed assessment based on information they collected across interviews, laboratory analysis, weather reports, information provided from the OPCW on-site mission, the OPCW fact-finding mission, and from external reports. The IIT also leveraged 3rd party reports to include reports from the Syrian government, other States, and individuals; these included social media and other secondary and tertiary sources which was used to support other data collection efforts. Following their detailed analysis, the IIT released their findings to the Director General of the OPCW. This report was then subsequently shared publicly in 2020 with the findings of the IIT confirming the Syrian government was responsible for the use of Sarin (a chemical weapon) in March of 2017 in Ltamenah, Syria (OPCW Investigatin and Identification Team, 2020).

Following the release of the report, the Russian Federation rejected the findings claiming the evidence for the analysis used falsified data and accused the OPCW of the propagation of disinformation targeting Syria (The Information And Press Department Of The Russian Ministry For Foreign Affairs, 2020). Based on this accusation from Russia, the OPCW and subsequently, the UN faced delays and heated debates regarding a response to the Syrian Chemical weapons use.

VSM: In mapping this organizational system into the defined VSM context (Figure 2), we envision the OPCW at-large as the organizational system with the IIT defined as the primary operational unit of focus (i.e., S1). As such – the Policy and Identity (S5) would be based on OPCW's policy to support the CWC and role in addressing allegations of chemical weapons use. Specifically, the IIT (our S1) is formally governed by the identity and policy of the OPCW (OPCW, 2021). The IIT would, via the command channel, be redirected based on specific decisions from the Director General.

Coordination (S2) within the OPCW to support the IIT objective is based on the interactions between the Director General, the Inspectorate Division and the Verification Division. These interactions support sharing of information between the IIT and the OPCW on-site mission, the OPCW fact-finding mission, and the OPCW information cell (each of which serve as separate operational units). This interaction also ensures coordination between the OPCW laboratories and other agencies performing specific analysis. For OPCW, coordination (S2) also ensures information storage and processing are based on OPCW-defined information standards and any analysis is compliant with the those defined by OPCW. These interactions are supported by the coordination channel (OPCW, 2021).

System Operations (S3), which is directly overseen by the Director General for IIT, supplies manpower needed to support the IIT mission as well as physical resources such as databases, analysis tools, and on-site logistics. As needed, the IIT can request added resources to support their mission via the resource bargaining and accountability channel; the IIT also provides information (feedback) (the S3*) regarding safety/security of the team (specifically the on-site members). These actions are coordinated directly though the Director General. The Director General also supports risk mitigation to ensure the safety/security of the on-site members and ensures data security (integrity and confidentiality) once collected data is within the OPCW system (OPCW, 2021).

System development and environmental scanning (S4) support to the IIT mission is more informal but includes providing third party reports to IIT. These include reports from the Syrian government, other Nation States, and individuals as well as social media and other secondary and tertiary sources which can be useful for the IIT (OPCW Investigatin and Identification Team, 2020), (OPCW, 2021).

The IIT (S1) receives and collects relevant information to include reports from other operational units, the S4, and direct inspection information. Information is stored based on the policies defined by the S2. Analysis process includes interpretation and information generation from collected data and data provided from other operational units; third party data is leveraged to support collection efforts but is not used directly in analysis. The analysis report released by the IIT is operational unit output that is shared with the OPCW Director General via the coordination channel. The Algedonic channel (a communication channel from the operational unit to the policy and identify reflecting urgent messages) reflects the ability of the IIT to directly signal issues or risks to the

Director General that they feel could impact the OPCW or the IIT mission such as changing on the ground threats or analysis discoveries that could have global security implications (OPCW Investigatin and Identification Team, 2020), (OPCW, 2021).

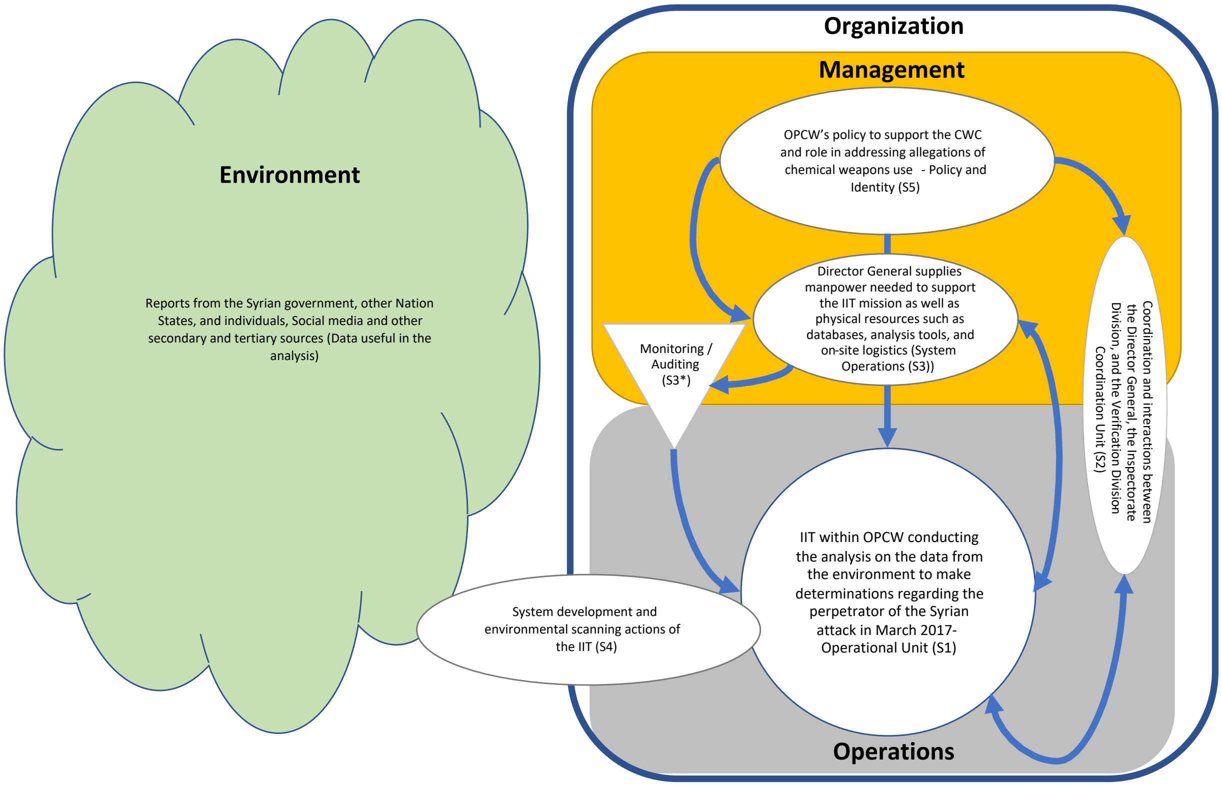

Figure 2. OPCW IIT operations reflected as a VSM model. This model mirrors the definitions provided in Table 1 as well as details above.

System gaps: Considering the information flow of the IIT, the systems defined in the VSM context, and the specific accusations by the Russian government regarding falsified information being used by the IIT (The Information And Press Department Of The Russian Ministry For Foreign Affairs, 2020), our team categorized the disinformation attack as one directly targeting the output of the operational unit. This is reflected in Figure 3.

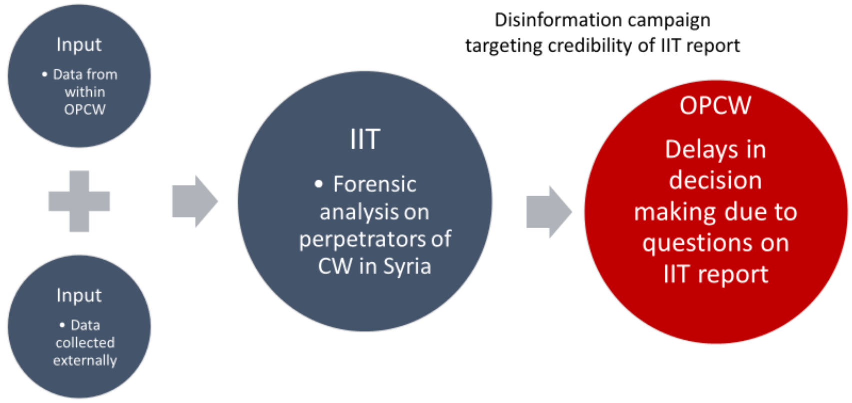

Figure 3. Disinformation Attack Target Witnessed by OPCW. In this case study, the attack was directed on the output of the IIT following its analysis, as this impacts the decision-making ability of the OPCW.

The IIT itself (S1) demonstrated the ability to validate, verify, and provide thoughtful consideration regarding the data prior to data analysis. The robustness of the IIT(S1) was supported by the operations function (S3), who ensured the day-to-day operations aligned with the OPCW processes, and the internal processes of the coordination (S2) and the environmental scanning function (S4) to support data collection and inputting into the S1 with sufficient metadata to allow confidence management. The system development (S4) also supported situational awareness. The operations (S3) enabled the implementation of innovation, such as more complex simulation and modeling, in the analysis process (identified by the S4) and the OPCW's formal information policies were ensured and communicated by the coordination subsystem (S2). However, while the IIT was itself not susceptible to disinformation, the results of their findings were put into question by Russia and subsequently other nations. Our team has characterized this system gap to be a failure in the communication channels focusing on the output of the IIT (S1) and a lack of understanding the relationship between the system (OPCW) and the environment (Russia), which should have been considered as part of the system development's (S4's) situational awareness – see Table 2 for a summary of the gaps.

GPEI

Background: The mission of GPEI is to eradicate the Sabin poliovirus from all environments across the globe. Polio is a virus that infects and is transmitted between human hosts only in humans and, while highly transmissible between the human hosts, the virus can be rendered unable to propagate in those who have been vaccinated. As with the Smallpox virus, it is possible to fully eradicate the virus through global vaccination efforts. There have been several efforts spearheaded by global (specifically the World Health Organization (WHO)) and national public health agencies to implement vaccination programs in areas where polio still is endemic. A primary element in the vaccination program is outreach and education regarding the virus and the benefits of the vaccine on its eradication. The WHO is reliant on local public health agencies, supported by their state and regional agencies, to implement the actual vaccination programs and work with the public to support their decisions to be vaccinated.

In the early 2000s, the WHO focused the GPEI on Africa, specifically Nigeria, where outbreaks reflected roughly 50% of those still witnessed worldwide (Global Polio Eradication Initiative, n.d.). GPEI provided information and resources to support the facilitation of local vaccination programs through state and local public health agencies. Nigeria's Kano state was one of the areas specifically targeted by the African GPEI effort, with the Kano Public Health agency (KPH) serving as a key partner for this effort.

Unfortunately, an active anti-polio campaign was launched by ethnonational extremists (Jegede, 2007) across Nigeria and provided falsified reports and biased anecdotal data (disinformation) to KPH and the Kano public. This disinformation created sufficient doubt around the information provided by GPEI, eventually leading the KPH to not participate in the vaccination program supported in the early 2000s (Jegede, 2007).

Unlike the OPCW case where it was widely accepted that no falsified data was included in the analysis, the data used by KPH in their analysis and subsequent decision-making included disinformation. This resulted in KPH withdrawal from the vaccine program and a massive delay in the public receiving vaccines. Based on this example, our team was interested in understanding how the organizational issues increased the susceptibility of the KPH to disinformation (Jegede, 2007).

VSM: Like OPCW, our team defined the GPEI in a VSM organization context. We considered the GPEI as the primary organizational system, with the KPH as the operational unit of focus. The policy and identity of the GPEI is based on its mission defined in 1988 by the World Health Assembly. From this mission the specific policy and identity defined as part of the GPEI oversight (S5) of the KPH is based on the 2003 focused effort to immunize more than 15 million children across west and central Africa. GPEI has very limited direct command of KPH, but guidance and support are filtered between the GPEI and the KPH via the African WHO field office reflecting the command channel (Global Polio Eradication Initiative, n.d.).

Coordination of information between the KPH and the African WHO field office (S2) is focused on coordination between the various other African local public health agencies that promote outreach activities. The African WHO field office is also the primary support for communication between involved entities (coordination channel) (Global Polio Eradication Initiative, n.d.).

The African WHO field office linked with the Nigerian Ministry of Health provides resources including manpower needed to support the KPH (S3), with specific funding for the KPH being directed by the Nigerian and Kano governments but supplemented by the African WHO field office and directly by the GPEI. Interactions between KPH and the Nigerian government allow for requesting additional resources to support their mission and provides information back (S3) regarding safety/security of the workforce (Global Polio Eradication Initiative, n.d.), (Jegede, 2007).

The KPH and the GPEI collect and share relevant information from the environment primarily via ad hoc processes. This environmental scanning (S4) includes the collection of information regarding outbreaks of polio across the globe, vaccination information, security issues, other public health issues, etc.

The KPH (S1) receives relevant information to support decision making internally regarding the eradication effort, makes determinations regarding how best to conduct public outreach, and implements the vaccination program. Also, the KPH can make the decision to not operate due to the limited direct governance over this operational unit by the GPEI.

System Gaps: Focusing on just the information used to support the work of the GPEI and KPH in the early 2000s (Jegede, 2007), our team identified the disinformation attack as one targeting the data collected from the environment, which was then used by the S1 (KPH) analysis and subsequent decision-making (Figure 3).

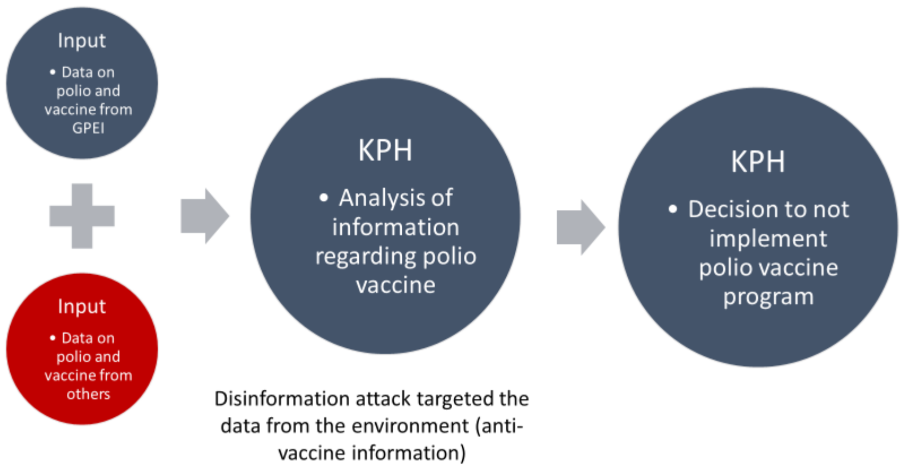

Figure 4. Disinformation Attack Target as Witnessed by GPEI. In this case study, the attack was directed on the input or data being pulled into the organization for analysis. As such, the organization used disinformation within their analysis impacting the results and subsequent decision making.

Unlike the OPCW exemplar, there was a clear lack of operational support within the KPH (S1) to ensure information inputs were valid and verifiable, and there was limited thoughtful consideration witnessed prior to inclusion in the data analysis. This reflects gaps within the operational support (S3) of the GPEI, as well as gaps regarding governance on polices to support data analysis (S2). Based on the disinformation being collected from the environment and included within the system, there were also limitations in environmental scanning processes (S4) – see Table 2 for a summary. Finally, as with the OPCW, the team also found a clear gap in situational awareness, i.e., understanding of the African politics and anti-western sentiment and the potential impacts to the GPEI.

Discussion

Considering the subset of VSM functions in concert with the system gaps, the team outlined specific requirements by each subsystem that would be needed to support resilience to disinformation. These have been outlined in the table below considering the influences within the VSM context (Table 2.)

Table 2. Subsystem considerations regarding overall system resilience to disinformation. Implications for each of the case studies are colored to reflect resilience (green), some gaps (yellow), or a lack of resilience (red).

VSM Subsystem (VSM Label)	*Requirements of subsystem to promote resilience*	*Observations: OPCW case*	*Observations: GPEI case*
Operational Unit (S1)	• Processes must ensure the input data is valid, verifiable, and thoughtfully considered prior to use in the analysis (e.g., confidence management of the data) • Must ensure sufficient resources to include workload balancing • Requires ability to implement innovation to support data management and analysis • Requires situational awareness to help support confidence management • Must ensure output aligns with mission needs and supports confidence management for the receiver	The IIT has defined processes to support confidence management on data inputs and appears to have sufficient resources, but the success of the disinformation attack (the Russian accusations) reflects a lack in situational awareness and measures to support confidence management in the output of the IIT	Neither the GPEI nor the KPH appear to have any confidence management processes regarding data inputs
Coordination (S2)	• Must ensure information analysis standards that promote confidence management • Must ensure inputs from other S1s are sufficiently robust and include metadata to support confidence management • Must ensure outputs from S1s are sufficiently robust and include metadata to support confidence management	Standards that support confidence have been defined by OPCW and these are reflected in the actions of the IIT and the handling of all the inputted data.	Coordination regarding the data inputs and implementation of standards for confidence management appear to be non-existent or ad hoc.
System Operations (S3)	• Must ensure resources are available to ensure sufficient data to information processes are robust to include workforce and equipment • Must ensure resources are available for the S1 to respond to changing situations and implementation of innovative ideas where needed	Resources are sufficient to support and ensure careful analysis, validation, storage, and thoughtfulness for all data inputs.	Resources provided to the KPH did not appear to include those to support information analysis or confidence management.
System Development (S4)	• Must ensure output from environmental scanning that is useful in the data to information process is sufficiently robust and include metadata to support confidence management • Must ensure S1 is aware of situations, which may impact the data to information conversion	The inputs from the environmental scanning reflect robustness to allow for the IIT to implement confidence management. However, there was a lack of awareness regarding the possible actions taken by Russia regarding the IIT's report.	Environmental scanning exists, but did not reflect processes to validate, verify, or thoughtful consideration of the data before use in analysis.
Policy and Identity (S5)	• Must ensure overall mission and information analysis needs are reflected in the S1 output	The IIT's mission was tightly constrained by the OPCW and reflected strong command and control of the operations.	The KPH's mission was not constrained by GPEI and as such there was no command or control reflected in the study.

Future Work

The VSM framework provides a powerful yet generalizable methodology for characterizing and evaluating organizational behaviors in the presence of disinformation. The team is working to extend these qualitative insights into quantitative, performance-based metrics that can be used to calculate the vulnerabilities of an organizational system to disinformation. The metrics align with the identified priority system subsystems – such as resources, situational awareness, and innovation. As the team progresses on this effort, we expect to define other metrics that may mirror specific system gaps within the subsystems or channels. The team is also pursuing modeling and simulation approaches (e.g., agent-based modeling (ABM)) to test and validate the utility of these metrics to inform resilience opportunities for organizational constructs. Although the VSM approach provides a powerful platform for understanding organizational functions and interactions, the actual assessment of organizational behaviors will require the ability to simulate different outcomes. Thus, alternate modeling approaches, such as the ABM will be important to support study of exemplar organizations that have experienced disinformation attacks. Outcomes from these ABMs can help validate which quantitative metrics have the largest influence on organizational resilience to disinformation and support assessment of metric transferability across different organizations.

Acknowledgements

This work was supported by the Laboratory Directed Research and Development program at Sandia National Laboratories, 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-NA0003525. SAND 2023-XXXX

References

Ashworth, M., & Carley, K. (2007). Can tools help unify organization theory? Perspectives on the state of computational modeling. *Computational and Mathematical Organization Theory, 13*, 89-111.

Global Polio Eradication Initiative. (n.d.). *Global Polio Eradication Initiative*. Retrieved 2022, from https://polioeradication.org/

Jegede, A. (2007). What Led to the Nigerian Boycott of the Polio Vaccination Campaign? *PLoS Med, 4*(3), 417-422.

Katina, P., & Keating, C. (2015). Extended Systems Principles. Unpublished Manuscript.

Keating, C. (2000). A systems-based methodology for structural analysis of health care operations. *Journal of Management in Medicine, 14*(3/4), 179-198.

Keating, C., & Katina, P. (2012). Prevalence of pathologies in systems of systems. *International Journal of Systems of Systems Engineering, 3*(3/4), 243-267.

Kirikova, M., & Pudane, M. (2013). Viable System Model Based Information Flows. In *New Trends in Databases and Information Systems : 17th East European Conference on Advances in Databases and Information Systems* (pp. 96-104). Springer International Publishing.

OPCW. (2021). *Investigation and Identification Team (IIT)*. (OPCW) Retrieved 2022, from https://www.opcw.org/iit

OPCW. (2021, April 12). *OPCW-UN Joint Investigative Mechanism (JIM)*. (OPCW) Retrieved 2022, from https://www.opcw.org/taxonomy/term/72

OPCW Investigatin and Identification Team. (2020). *First Report By The Opcw Investigation And Identification Team Pursuant To Paragraph 10 Of Decision C-Ss-4/Dec.3 "Addressing The Threat From Chemical Weapons Use" Ltamenah (Syrian Arab Republic) 24, 25, And 30 March 2017.* The Hague: OPCW.

Perez, R. (2012). *Design and Diagnosis for Sustainable Organizations.* Berlin: Springer.

Rezaee, Z., Azar, A., Ba Erz, A., & Nayeri, M. (2019). Application of Viable System Model in Diagnosis of Organizational Structure. *Systemic Practice and Action Research, 32*(3).

Rodríguez-Fernández. (2019). *Disinformation and organisational communication: A study of.* http://www.revistalatinacs.org/074paper/1406/89en.html: Revista Latina de Comunicación Social.

Socialtrendly INC. (2021). *History Of Misinformation*. (Blackbird.AI) Retrieved 2021, from https://www.blackbird.ai/history-of-misinformation/

The Information And Press Department Of The Russian Ministry For Foreign Affairs. (2020). *Russian Federation Comment By The Information And Press Department Of The Russian Ministry For Foreign Affairs On The Release Of The First Report By The OPCW Investigation And Identification Team.* The Hague: OPCW.

United Nations. (2020, Nov 5). Syria: No justification for chemical weapon use 'under any circumstances' – UN disarmament chief. *UN News*, p. https://news.un.org/en/story/2020/11/1077002.

United Nations. (2021, May 6). Nearly 8 years on, 'gaps, inconsistencies, discrepancies' remain over Syria chemical weapons declaration. *UN News*, p. https://news.un.org/en/story/2021/05/1091462.

Wachtel, A., Jones, K., Baca, M., O'Neill-Carrillo, E., & DeMenno, M. (2020). *Sandia's Integrated Methodology for Energy and Infrastructure Resilience Analysis.* Albuquerque: Sandia National Laboratories.

Williams, B., & Hammelbrunner, R. (2010). *Systems Concepts in Action: A Practitions's Toolkit.* California: Stanford University Press.