Digital systems in High-Reliability Organizations: balancing mindfulness and mindlessness

Paolo Spagnoletti[a,b], Andrea Salvi[a]

[a] *Department of Business and Management, Luiss University, Rome, Italy*
[b] *Department of Information Systems, University of Adger, Norway*

Abstract
High-Reliability Organizations (HRO) operate in a nearly error-free manner in an uncertain environment characterized by high risks and equally high stakes. Collective mindfulness is a key capability of HRO. The literature has successfully identified both individual and organizational processes to achieve collective mindfulness. In this position paper we investigate the role of digital systems in HRO. We compare the operative functions of organizations in conjunction with digital technologies to lay the foundations for an empirical analysis on the structural determinants of "mindfulness in action". We identify alternative scenarios of mindfulness and mindlessness as a first step towards the development of a contingency model for digital enabled collective mindfulness. Specifically, we provide preliminary insights from the discussion of two cases: a military command and control system, and an inter-organizational platform for fraud-detection. We contribute to the sociotechnical literature by discussing the properties of collective mindfulness in layered settings of human operations and digital operations.

Keywords
HRO, resilience, mindfulness, digital systems

1. Introduction

High-Reliability Organizations (HRO) operate in a nearly error-free manner in an uncertain environment characterized by high risks and equally high stakes [1]. Collective mindfulness is a key capability of HRO. The literature has successfully identified both individual and organizational processes to achieve collective mindfulness. In this position paper we investigate the role of digital systems in HRO. In particular, we compare the operative functions of organizations in conjunction with digital technologies in order to lay the foundations for an empirical analysis on the structural determinants of "mindfulness in action" [2]. We identify alternative scenarios of mindfulness and mindlessness as a first step towards the development of a contingency model for digital enabled collective mindfulness.

HROs, in fact, are not routine-based entities. Their peculiar features stem from an efficient capacity of detecting and correcting errors originated from uncertainty [1] often referred to as "organizational mindfulness processes" [3], [4]. A plethora of qualitative studies have looked at near-error-free organizing in critical scenarios (e.g. first responders [5]) and delineated the differences between HROs and traditional organizations as represented by a stark inclination towards reliability and resilience rather than focusing on pure efficiency [6], [7]. This cognitive mindset is the by-product of five systematic characteristics: chronic preoccupation with failure, reluctance to simplify, sensitivity to operations, commitment to resilience and deference to expertise [8]. Furthermore, frontline organisations exhibit a sixth trait identified as "comfort with uncertainty and chaos" [2]. The interplay between these characteristics creates the foundations of mindfulness equipping HROs with rich awareness of discriminatory detail and capacity for action [2], [8].

Proceedings of the 6th International Workshop on Socio-Technical Perspective in IS Development (STPIS 2020), June 8-9, 2020
EMAIL: pspagnoletti@luiss.it (A. 1); asalvi@luiss.it (A. 2)
ORCID: 0000-0003-1950-368X (A. 1); 0000-0002-3583-0114 (A. 2)

In this contribution, by looking at this framework, we observe how two operative functions of organizations have been able to harness systems making use of their affordances as enablers of collective mindfulness. We define the latter as a state whereby high reliability organizing are enabled in the form of rich awareness of discriminatory detail, heedful interrelations and capacity for action (Fraher et al., 2017; Weick & Sutcliffe, 2006). It is constituted by processes of "sensemaking" (Weick & Roberts, 1993) that enable actions dynamic, uncertain and extreme environments (Christianson & Barton, 2020). There is a vast literature that acknowledges the role of information systems in emergency response and extreme-contexts preparedness [9]–[11]. Yet, less attention has been given to the interactions of "mindless" digital systems with the "human" organizational structures of HROs [4]. Here we argue that when opportunely devised and integrated in the respective sociotechnical system of organizations, they are powerful mediums of coordination and can help achieve a state of "mindfulness in action". The implementation of Blue Force Tracking 2 (BFT) by the US military provides a prime example of our thesis (Section 2). Furthermore, we present the inter-organizational case of EU-OF2CEN (European Union Online Fraud Cyber -Center Expert Network)(Section 4). Finally, we will discuss their features using the framework provided Salovaara et al (2019) and use their case of a malware-protection company as a baseline for a purely digital HRO. We claim that the increased awareness resulting from a "human-serving" or "human-driven" design and implementation of digital systems allows for a more efficient "switching" between structure and flexibilities depending on the challenges that actors face during their operations.

We contribute to the sociotechnical literature by discussing the properties of collective mindfulness in layered settings of human operations and digital operations. Contemporaneously it sets the foundations for a future design theory work that aim to contribute to the literature on HRO by investigating the interplay of mindfulness and mindlessness in a broader sample of organizations.

2. Digital enabled command and control systems: military organizations and tracking technologies.

Operative military organizations are prime examples of HROs as they need to operate amid the "fog of war". They operate under special conditions characterized by extreme events with high potential magnitude of consequences for both organizational members and other actors. Furthermore, they engage with extreme events less frequently as compared to other HRO and for longer timespans. These factors require adopting an approach that consider crisis as a process rather than as a single event [12]. That is, frontline military personnel engage with crisis scenario, they need to embrace an augmented High Reliability mindset. In fact, military organization operate under austere conditions or time constraints that do not allow personnel replacements: team members must be ready to step up and take the role of other team members or assume formal leadership positions if leaders are lost. This posits the need for preventive measures to increase the High Reliability mindset including redundancies in training and cross-functional training.

Therefore, we observe a constant balancing between structure and flexibility [13] as required by the contingencies of the battlefield. This balancing is achieved by the adoption of the so-called doctrine of Mission Command. The latter solves the "entrenchment problem" of over-reliance on Standard Operating Procedures (SOPs) [4]. It also embraces the six hallmarks of HROs ultimately leading to tactical awareness apt to striving for graceful coping with surprises and learning from mistakes [4].

Military operations – even more so in the frontline – are mainly human-centric. Decisions need to be taken at different levels to build a strategic and tactical address vis-à-vis the challenges presented by the battlefield. While, as discussed above, the entrenchment problem is solved by mission-oriented organizing, the emergence and implementation of advanced digital systems in military organization may severely hamper the tactical dimension of these organizations. A purely vertical digitalized command and control structure may in fact favour "mindlessness" over "mindfulness" due to over-reliance on "mindless" systems. Yet, as empirical evidence suggests, military organizations have been able to layer digital and human operations to be integrated. In this way, personnel – while still retaining

his primacy – can make use of such technologies to enhance their operative awareness and – in turn – perfect the digital systems through human inputs. In this short paper, we will discuss the case of the Blue Force Tracker 2, which has seen a widespread adoption in many military organizations.

The BFT is a Command and Control system: its main functions is that of providing the command centre with the GPS coordinates and real-time tracking of troops' movements. Furthermore, each deployed operator can input custom entries (e.g. enemy units, obstacles) and visualize the presence of other units. The first terminals were fitted to transport vehicles allowing for a more agile coordination of dispersed units [14]. The affordance belying this system is that of allowing for a more agile manoeuvring at the tactical level vis-à-vis the fine-grained disaggregated data in harmony with the doctrine of Mission Command. This is achieved through the union of situational awareness and command and control information [14] The estimated marginal effect of its adoption resulted in a reduction of Blue-on-Blue events between 24% and 12% in the Gulf War, increasing situational awareness of commanders not only towards enemy forces, but even more so towards movement of allied ones [15]. Through this system, platoon-commanders on the battlefield and leaders in the Tactical Operation Centres can act concurrently towards a unified goal. There is a vast scholarly work on decision-making that framed its core capability as "combat identification" (CID) [16]. The latter is composed by processes that ameliorate the management of available resources, maximize the utility of specific actions through more agile operations and ultimately fosters awareness by signaling the position of allied forces and foes to minimize the occurrence of blue-on-blue events[1] [17].

The integration between the digital component and the human one is made possible by the sociotechnical setting and the command model. In detail, the mission-oriented approach, and the diluted model of leadership of operations, allow for a widespread "responsibilization" of operators. Digital Systems are used to increase and augment the awareness of those on the battlefield instead of replacing their decision-making. In fact, excessive reliance on digital systems may be highly problematic in operative functions of military organizations. As a notable example: accounts from real campaign describe as General Franks of CENTCOM in 2003 used the BFT to "punish" idled units [18]. Furthermore, evidence drawn from surveys recount episodes whereby the BFT was used to issue direct orders. Specifically, with a clear picture of the situation on the battlefields, HQs were often able to tactically maneuver Marine platoons [19] de-facto centralizing the leadership of operations. Even more importantly, these systems are profoundly reliant on data. Simulations studies on BFT have shown how a "timely and flawless transmission" of data is key to warrant a positive effect on maneuvering and awareness [16]. These works therefore propose that over-reliance on digital systems may severely undermine correct combat identification judgments.

What we claim is thus that the implementation of digital systems does not imply a purely mindless structure. Quite the opposite, if properly integrated in the sociotechnical fabric of an organization, they can be valuable driver of mindfulness.

3. EU-OF2CEN: an inter-organization anti-fraud system.

The banking and financial sectors have seen increasing levels of cyber-dependency due to the digital-intensive nature of their products. This dependency, have shaped new horizons of risks stemming from the potential material and societal damage [20]. Deceptions and frauds are particularly common in these sectors and malicious actors have found a variety of opportunities stemming from the open-ended nature of digital infrastructures [21]. This posits the need for inter-organization efforts towards collaborative monitoring systems [22] able to contrast threats and foster information sharing between actors sharing the same risks and similar stakes.

[1] Friendly fire events in NATO nomenclature.

In this case, we focus on the EU-OF2CEN (European Union Online Fraud Cyber -Center Expert Network). It is a project started by the Italian Police and financed by the European Union, aimed at contrasting financial cybercrime. It takes the form of a platform able to collect real time data through secure communication channels. Specifically, banks and police authorities report suspicious transactions taking place on the Internet. The platform allows to process these data, analyze them and share the results with the partners. The EU-OF2CEN de-facto constitutes a collaborative monitoring system striving for reliable early warnings of possible criminal activities.

Such ensemble of tools provides an inter-organization High Reliability platform that brings several benefits to the partners. It enhances financial institutions' ability to assess the nature of bank movements for the subsequent implementation of effective actions to prevent or contain fraud or money laundering. Similarly, Law Enforcement Agencies (LEAs) can make use of the data and of the aggregated data for investigations. Therefore, LEAs can make use of the output of the "mindless platform" to facilitate the identification of the responsible and to investigate the nature of the crime. Overall, the peculiar Public Private Partnership (PPP) between Europol, LEAs and banks, strives to the creation of a common mindfulness towards the criminal trends in the financial and cyber domain through the insights of a mindless data-driven system. We can therefore witness an increase common awareness which in turn fosters cooperation towards concrete and timely actions in the operative domain.

In sum, with EU-OF2CEN we observe how a mindless digital platform – constrained by the frame problem – can augment the reliability and the information-sharing in a set of organizations. Thus, the platform works on running the main operations in turn increasing the awareness of the human actors and in enabling a powerful mean of communication between them. Human control in this context can help the digital tool to overcome its framing limit. Again, we observe how the layering of human driven and digital driven operations can overcome the main pitfalls of the two approaches.

4. Comparison and Discussion

In this brief paper we have presented a preliminary framework for analyzing the effect of digital systems in HRO. As shown in **Table 1**, there are three dimensions for analyzing operations in this context. The nature of the operation as discussed, can be either human-based or digital while the nature of the cognition can be Mindful or Mindless. Finally, the purpose can be purely epistemic or pragmatic.

Table 1
Three Dimensions for Analysing High-Reliability Digital Operations. Reproduced from Salovaara et al (2019, p. 561)

Feature	Feature Type	
Nature of Operation	*Human-based:* approximate, error-prone, limited by memory capacity and processing speed, of varying precision, context-sensitive	*Digital*: exact, transferable, editable and programmable via expression of binary data
Nature of Cognition	*Mindful*: heedful, with anticipation of surprises and prioritization of safety in operations, unconstrained by the frame problem	*Mindless*: constrained by the frame problem via algorithm-use or reliance on highly structured routines
Purpose	*Epistemic*: interpreting and	*Pragmatic*: performing decision-making and acting

	analysing information

The examples provided suggest that – among other factors - what drives an HRO towards the maximization of reliability is the layering and the interactions between the human and the digital. We claim, as a preliminary step towards a broader analysis, that the ordering of the layering matters in shaping the processes that lead to a status of reliability through mindfulness.

In **Table 2** we report our examples of BFT and EU-OF2CEN using the case of F-Secure – a malware-protection digital company – as baseline. The case of F-Secure has been thoroughly analyzed by Salovaara et al (2019) with a particular attention to the layering of mindful and mindless operations. Furthermore, the latter is a fully digital organizations: it is expected to face more constraints vis-à-vis the framing company as compared to hybrid operations from our cases. Specifically, we classified the three digital systems based on the nature of operations, nature of the cognition and digital features proposed by Grover (2020). The latter are:

- *Embeddedness:* integration of the physical and the digital to create expansion for the affordances.
- *Decoupling:* no – or shallow - linkage between the digital content and the container.
- *Representation:* connections and operations can be represented in digital form [23].

As for the nature of operation, we departed from the classification proposed in Table 1 to portray the interactions and the layered nature of the human/digital relation. The same applies to the nature of the cognition whereby we want to highlight how a mindless platform can surpass the framing problem throughout human induced mindfulness.

Table 2
Comparison between digital entities based on nature of operation, nature of cognition and digital features.

Digital entities	Nature of operation	Nature of cognition	Digital features
BFT	Human-based with digital enhancement	Digital enhanced Mindfulness	Embeddedness, decoupling, representation
EU-OF2CEN	Digital based with human enhancement	Mindless platform with human induced mindfulness	Decoupling, representation
F-SECURE	Digital based with human enhancement	Mindless platform with human induced mindfulness	Decoupling, representation

In the case of the military organizations, digital control systems enhance mindfulness of human operators, which retain the pre-eminence in terms of actorness and can benefit from the augmented awareness given by these tools. We suspect that this equilibrium strongly associated with the embeddedness of monitoring systems – such as the BFT – in the physical world. As for the case of EU-OF2CEN, we observe the opposite layering: a purely digital "mindless" platform run the core operations which are then validated and scrutinized by human-driven functions. This pattern is fairly similar to the F-Secure case. Even though operations start and are mainly ran by a digital platform, collective mindfulness within the respective organization is induced by the human "sitting in the back-seat" [4]. All in all, we claim that the increased awareness resulting from a "human-serving" and "human-driven" designs and implementations of digital systems allows for a more efficient "switching" between structure and flexibility.

This analysis, albeit purely positional, aim to highlight the emergent issue of the interactions between mindfulness and mindlessness in HRO vis-à-vis their digital systems. We contribute to the sociotechnical literature by discussing some of the basic properties of collective mindfulness in

layered settings of human operations and digital operations. Further work will carry on the analysis of the interactions between different operative functions, systematizing the basic comparisons proposed in this first contribution. Furthermore, we aim to study in more detail the association between digital features and the nature of operation and cognition. All in all, the increased empirical understanding together with the link between digital features and nature of HRO operations should lay the foundations for the development of a contingency model for digital enabled collective mindfulness.

5. Limitations and Assumptions

This paper constitutes a further step towards the analysis of mindful and mindless systems in HRO. We acknowledge the presence of several limitations, partly due to the positional nature of the integration. In first place, in this context we assume that digital operations suffer from the so-called frame problem as discussed by Salovaara (2019). That is, algorithms that animate these systems cannot really adapt to events or environments that are not pre-identified by their creators "cognitive frames". This is key to understand the need for balance between mindfulness and mindlessness. Digital systems may perhaps achieve higher levels of reliability, but such a performance is heavily dependent upon its' original framing.

6. References

[1] K. E. Weick and K. H. Roberts, "Collective mind in organizations: Heedful interrelating on flight decks," *Adm. Sci. Q.*, pp. 357–381, 1993.

[2] A. L. Fraher, L. J. Branicki, and K. Grint, "Mindfulness in Action: Discovering How U.S. Navy Seals Build Capacity for Mindfulness in High-Reliability Organizations (HROs)," *Acad. Manag. Discov.*, vol. 3, no. 3, pp. 239–261, Sep. 2017, doi: 10.5465/amd.2014.0146.

[3] A. Mohun and S. D. Sagan, "The Limits of Safety: Organizations, Accidents, and Nuclear Weapons," *Technol. Cult.*, 1995, doi: 10.2307/3106400.

[4] A. Salovaara, K. Lyytinen, and E. Penttinen, "High reliability in digital organizing: Mindlessness, the frame problem, and digital operations," *MIS Q. Manag. Inf. Syst.*, 2019, doi: 10.25300/MISQ/2019/14577.

[5] G. A. Bigley and K. H. Roberts, "The Incident Command System: High-Reliability Organizing for Complex and Volatile Task Environments," *Acad. Manag. J.*, vol. 44, no. 6, pp. 1281–1299, 2001.

[6] K. M. Sutcliffe and T. J. Vogus, "Organizing for resilience," *Posit. Organ. Scholarsh. Found. a new Discip.*, vol. 94, p. 110, 2003.

[7] T. J. Vogus and K. M. Sutcliffe, "Organizational mindfulness and mindful organizing: A reconciliation and path forward," *Acad. Manag. Learn. Educ.*, vol. 11, no. 4, pp. 722–735, 2012.

[8] K. E. Weick and K. M. Sutcliffe, "Mindfulness and the quality of organizational attention," *Organ. Sci.*, vol. 17, no. 4, pp. 514–524, 2006.

[9] I. Aedo, P. D\'\iaz, J. M. Carroll, G. Convertino, and M. B. Rosson, "End-user oriented strategies to facilitate multi-organizational adoption of emergency management information systems," *Inf. Process. Manag.*, vol. 46, no. 1, pp. 11–21, 2010.

[10] B. Van De Walle, M. Turoff, and S. R. Hiltz, *Information systems for emergency management*. Routledge, 2014.

[11] M. Turoff, M. Chumer, B. Van de Walle, and X. Yao, "The design of a dynamic emergency response management information systems (DERMIS)," *J. Inf. Technol. Theory Appl.*, vol. 5, no. 4, pp. 1–35, 2012.

[12] T. A. Williams, D. A. Gruber, K. M. Sutcliffe, D. A. Shepherd, and E. Y. Zhao, "Organizational

response to adversity: Fusing crisis management and resilience research streams," *Acad. Manag. Ann.*, vol. 11, no. 2, pp. 733–769, Jun. 2017, doi: 10.5465/annals.2015.0134.

[13] A. Salovaara, K. Lyytinen, and E. Penttinen, "Flexibility vs. Structure: How to Manage Reliably Continuously Emerging Threats in Malware Protection," in *2015 48th Hawaii International Conference on System Sciences*, 2015, pp. 4980–4989.

[14] K. R. Chevli *et al.*, "Blue Force Tracking Network Modeling and Simulation," in *MILCOM 2006 - 2006 IEEE Military Communications conference*, Oct. 2006, pp. 1–7, doi: 10.1109/MILCOM.2006.302050.

[15] M. Augier, T. Knudsen, and R. M. McNab, "Advancing the field of organizations through the study of military organizations," *Ind. Corp. Chang.*, vol. 23, no. 6, pp. 1417–1444, Feb. 2014, doi: 10.1093/icc/dtt059.

[16] D. J. Bryant and D. G. Smith, "Impact of blue force tracking on combat identification judgments," *Hum. Factors*, vol. 55, no. 1, pp. 75–89, 2013.

[17] L. Doton, "Integrating technology to reduce fratricide," 1996.

[18] M. R. Gordon and B. E. Trainor, *Cobra II: The Inside Story of the Invasion and Occupation of Iraq*. New York: Pantheon, 2006.

[19] M. J. Dreier and J. S. Birgl, *Analysis of Marine Corps Tactical Level Command and Control and Decision Making Utilizing FBCB2-BFT*. Monterey, CA: Naval Postgraduate School, 2010.

[20] R. Baskerville, P. Spagnoletti, and J. Kim, "Incident-centered information security: Managing a strategic balance between prevention and response," *Inf. Manag.*, vol. 51, no. 1, pp. 138–151, Jan. 2014, doi: 10.1016/j.im.2013.11.004.

[21] S. Grazioli and S. L. Jarvenpaa, "Consumer and Business Deception on the Internet: Content Analysis of Documentary Evidence," *Int. J. Electron. Commer.*, vol. 7, no. 4, pp. 93–118, 2003, doi: Article.

[22] S. Gregor and A. R. Hevner, "Positioning and Presenting Design Science Research for Maximum Impact," *MIS Q.*, vol. 37, no. 2, pp. 337–355, 2013.

[23] I. Gregory, D. DeBats, and D. Lafreniere, "Introduction to part IV," *The Routledge Companion to Spatial History*. Edward Elgar Publishing, pp. 351–352, 2018, doi: 10.4324/9781315099781.