BOOK CHAPTER | *"PARS – Making things Happen"*

Phase-Oriented Advice and Review Structure (PARS) for Digital Forensic Investigations

Aliloulaye Tchaou
Digital Forensics and Cyber Security Graduate Programme
Department of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mail: aliloulay@gmail.com
Phone: +233597238085

ABSTRACT

The PARS is the first documented peer review methodology for the digital forensics field, a six staged approach designed to formally support organizations and their staff in their goal of facilitating effective peer review of digital forensic work, from investigative tasks to forensic activities and forensic analysis processes (Pollitt et al., 2018). This assignment discusses how the PARS methodology can be implemented, and the available options and mechanisms available to ease the interpretation of this model into existing practices. Both the early 'Advisor' and later 'Reviewer' roles in PARS are discussed and their requirements and expectations are defined.

Keywords: Digital forensics, Peer review, Digital evidence, Quality assurance, Forensic science Multi-staged Rview, Multi-person Review

BOOK Chapter | Research Nexus in IT, Law, Cyber Security & Forensics. Open Access. Distributed Free

Citation: Aliloulaye Tchaou (2022): Phase-Oriented Advice and Review Structure (PARS) for Digital Forensic Investigations
Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 173-180
www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P28

1. INTRODUCTION

PARS is a peer review methodology designed for rollout across the digital forensic discipline to support organizations in the task of implementing a system for reviewing practitioner work to uphold and maintain acceptable quality standards. PARS is aimed at supporting any type of DF (digital forensic) organization from DF laboratory environments or smaller DF units, private or public. The structure of PARS is described in detail and the requirements of each component mapped, which facilitates a partial or stepwise implementation.

1.1 Background to the Study

Arguably, a 'traditional' styled peer review process in DF could be considered a singular entity, which takes place in the closing stage of an investigation. In essence, peer review is often thought of as the final (and in some cases, primary) quality control (QC) check undertaken by an organization. As a result, it is naturally considered as a single entity; a process of checking 'everything' a practitioner has done following the close of their work on a given case.

The problem with this approach is arguably threefold:

1. *Efficiency… or Inefficiency*: To understand the impact that a traditional styled peer review has upon efficiency, one must consider a peer review, which uncovers significant flaws in each digital forensic investigation process. In such cases, further fundamental work may be required, which could include the completion of additional (or re-running of) processes or the undertaking of supplementary testing.

2. *Reactive rather than preventative*: Given that traditional peer reviews take place at the end of the DF process, they are by their very nature a reactive process. They are designed to evaluate in their entirety the complete investigative process and everything that has been generated as a result. In comparison, a peer review which occurs earlier in the investigative process, and at defined stages, can rectify any apparent error earlier, and in some instances prevent any error from impacting on further aspects of a case (as noted above).

3. *Too much to review*: A traditional peer review must evaluate all the investigatory process that has taken place. This raises the question as to whether this is too big of a task to undertake in one sitting, where a divide and conquer approach to the peer review process allows more manageable sub-reviews to take place, arguably increasing the chance of identifying errors.

The PARS approach presented in this work aligns the peer review process to the typical stages of a DF investigation, widely documented in academic literature (Köhn et al., 2006; Casey, 2011; Agarwal et al., 2011; Jafari and Satti, 2015). Fig. 1 shows the peer review process staged across the DF investigation process. PARS is inspired by the procedure for periodic review of investigations, described in the ACPO Murder Investigation Manual (2006), and several of the force-level policy documents by National Centre for Policing Excellence (2005 etc. - see also Savage and Milne 2011).

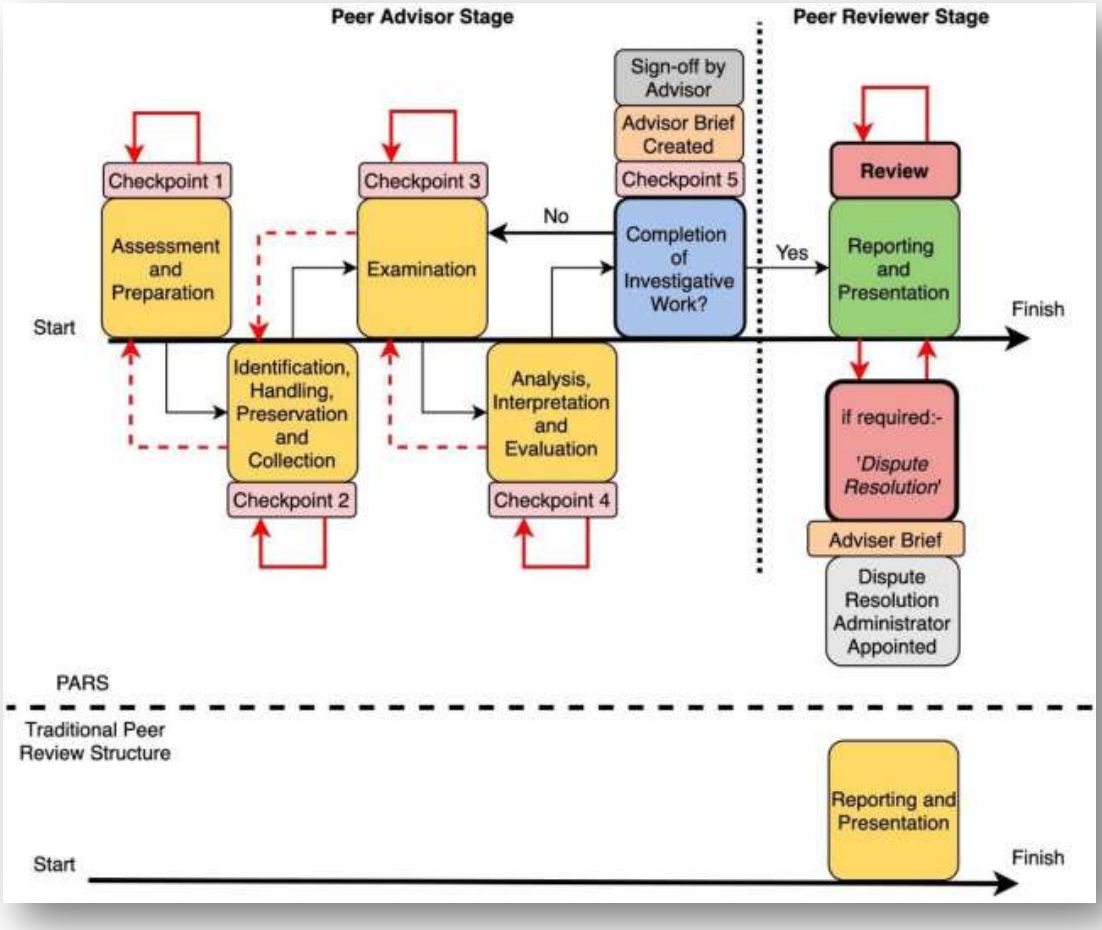

Fig. 1. PARS Vs. Traditional peer review models.
Source: The Phase-oriented Advice and Review Structure (PARS) for digital forensic investigations, Nina Sunde, Graeme Horsman

The PARS approach makes two fundamental changes to traditional peer review. It is:

(1) Multi-staged with the requirement for 'dispute resolution' procedures, and
(2) Multi-person divided into two roles ('Advisor' and the 'Reviewer'):

1.2 Multi-Staged Review

The proposed review structure consists of five 'stages', enforcing an iterative approach to peer review. We propose that each investigation should pass through four 'Advisor Checkpoints' and a final 'Review' (discussed below). This approach closely aligns to the main steps a practitioner will address when conducting casework, which are often considered critical milestones in all investigatory processes. In doing so, the review is a constant system of checks and verification to prevent not only a singular error from occurring, but to then stop any such error from impacting further investigative work. The multi-stages approach is designed to lessen the burden of the review by compartmentalizing the review into more frequent, but arguably manageable stages.

1.3 Multi-Person Review

Whilst counter arguments to such a proposal will lie with resourcing concerns, it is argued that an effective review must be one which is undertaken through multiple agents. Here, a proposal is made to divide the peer review burden between two entities, one who supplements and guides the primary investigator through their casework, followed by a second individual who is independent to the investigative process, who reviews the case in its entirety, often via a review of the written report. Dividing the task between two roles is done for two main reasons. First, advising through Checkpoints and performing peer review of the final report would be a substantial workload for a single person, with a risk of reduced quality due to a too burdensome process. Second, separating the advice and review tasks is justified with the risk of cognitive bias. If the same person should give advice and perform peer review, they would not review with 'fresh eyes', and would be biased from what they already knew about the DF investigation of the case. Since they already have invested effort to enhance the quality of the result through the peer advice stage, a risk of irrational escalation of commitment (Staw, 1981), which may reduce the ability to sufficiently critical during the peer review stage. In essence, we are proposing that the roles of 'Advisor' and 'Reviewer' (which we introduce in detail below) are two separate individuals.

The 'Advisor' and 'Reviewer' roles: The distinction between the 'Advisor' and 'Reviewer' roles is that of criticality and position in the review process. During the early stages of the PARS review (1–4), those engaging in the peer review process are doing so as a 'critical friend'. Their role is that of advice-giver, considering the facts of a given case and the approach of the practitioner, offering recommendations for approaching their tasks and where necessary steering the investigative process. Whilst those advising at each stage will still check critical facts and processes (seen predominantly at stages 1 & 2), the role is to feed-forward, where advice should look to increase the comprehensiveness of the investigation. The Advisor role is proposed to be undertaken by one individual who can guide the practitioner through each of the five Checkpoints (see Fig. 1).

2. RELATED LITERATURE

The PARS model is aimed at all organizations carrying out DF investigatory work, encompassing both private and public sector DF laboratories and DF units. Typically, most DF casework will follow a standardized investigative methodology, but often this methodology omits recognition of the need to peer review. Therefore, as a first requirement, organizations must ensure that peer review is formally acknowledged in their existing practice models and given the time and resources to effectively undertake this practice.

Extending the traditional DF investigative model: Over the last 15 years there have been multiple investigative models proposed for DF (see scoping reviews from Kohn et al. (2013) and Du et al.'s (2017) highlighting many of those in existence), and many maintain at their core, the same main aspects of an investigation. Whilst not all (see, for example the acknowledgement of a review stage by Agarwal et al. (2011)), many do not explicitly recognize the requirement for a stage involving robust peer review as part of the DF investigatory process or omit to discuss the implementation or requirements of it. As a result, this work opts to consolidate existing framework discussions and offers a clear requirement for peer review to be part of a 7 stage DF investigative process, shown in Fig. 2.

If we consider PARS as a compartmentalized process, each element must be examined:

- Assessment and preparation
- Identification, handling, preservation, and collection
- Examination
- Analysis, interpretation, and evaluation
- Investigative work complete?

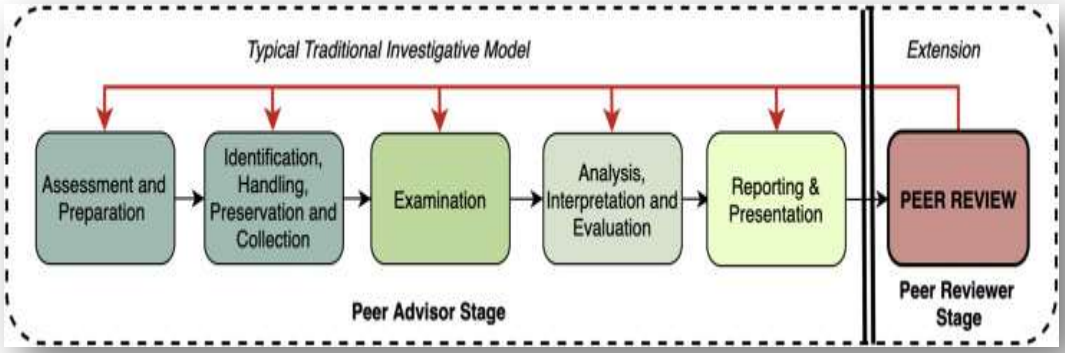

Fig. 2. The proposed investigative model incorporating peer review.
Source: The Phase-oriented Advice and Review Structure (PARS) for digital forensic investigations, Nina Sunde, Graeme Horsman

3. IMPLICATIONS FOR CYBER SAFETY IN AFRICA AS WELL AS IMPLICATIONS FOR PRACTICE, RESEARCH, AND POLICIES

In Africa, many countries have seen a rise in reports of digital threats and malicious cyber activities. The results include sabotaged public infrastructure, losses from digital fraud and illicit financial flows, and national security breaches involving espionage and intelligence theft by militant groups (*Source: Mustapha Saeed and Sone Osakwe, Researchers at the Centre for the Study of the Economies of Africa*).

Our research at the Centre for the Study of the Economics of Africa (CSEA) highlights several ways to improve cybersecurity across the continent.

Specifically, decision-makers need to take the following actions:

- Increase public awareness campaigns to encourage behavioral change, such that Internet users are aware of possible cyberthreats and know to adopt preventive measures.
- Invest in building up cybersecurity capabilities and technologies to detect and mitigate cybercrime.
- Devote more resources to setting up and equipping CIRTs, ensuring adequate capacity to monitor and respond to incident reports.
- Legislate efficient procedures for investigating and prosecuting cybercrime, thereby to deter cybercriminals.

- Commit to enforcing robust legislation that governs cyber activities and protects digital rights.
- Where cybersecurity strategies are already in place, ensure better coordination and thus stronger implementation.
- Strengthen partnerships between domestic stakeholders – public and private – to encourage the sharing of intelligence on potential threats and collaboration to find lasting solutions.
- Enhance regional cooperation among African states to ensure a united voice when negotiating over multilateral cybersecurity standards.
- Adopt a collective, region-wide approach that encourages peer learning and knowledge exchange.

4. RESEARCH GAPS/FINDINGS

Many different explanations and development have been left for the future due to lack of time. Future work concerns deeper analysis of PARS model, role progression in PARS, PARS review, the cost of implementing PARS and PARS efficiency.

5. CONCLUSION

The forensic science community have universally adopted peer review, and very often in the form of verification, as an essential part of systems for quality management and error mitigation. PARS approaches peer review with a more methodological comprehensive strategy to facilitate a robust peer review. PARS is a flexible framework which can be compartmentalized and implemented over time, when an organization finds it appropriate to engage in more of the elements it contains. It is argued that a shift to the systematic implementation of advice and review of a limited number of cases is a first step towards effective peer review. We argue that an investment in the robust peer review methodology offered by PARS will provide long-term quality assurance benefits for an organization.

6. RECOMMENDATION FOR POLICY AND PRACTICES

There is no doubt that reviewing work will involve a cost to the organization in the form of time and resources, and this is acknowledged here. It requires vast knowledge not only to understand digital evidence, but also to be able to effectively question the evidence itself, and the trustworthiness of the process that resulted in it. We question whether there is sufficient knowledge in judicial systems to challenge the quality of digital evidence, which entails the knowledge to ask the right questions and understand the implications of the answers.

Therefore, it is imperative that these checks are undertaken before any investigative work reaches this stage. Preventing errors through providing advice at the defined checkpoints and increasing ability to detect erroneous and misleading conclusions through implementing the Peer Review Hierarchy, is in our opinion a good investment in quality and an important measure for safeguarding the rule of law.

7. DIRECTION FOR FUTURE WORKS

To gain knowledge about the effect of advice and review on the quality of DF investigative work, the implementation of PARS should be evaluated, and itself subject to review. In essence, this series of work has designed and proposed PARS, and the next planned logical stage of our work is to evaluate the implementation of PARS by actual organizations. In addition, more knowledge is required regarding where in the DF process errors are most likely to occur, and which measures are best positioned to uncover or prevent these. Establishing this information will allow the refinement of the PARS review process. More information about the relationship between variables such as case type, practitioner experience and risk factors vs the scope of a review (level in the Peer Review Hierarchy) will also provide support for the continued development of effective peer review practices

REFERENCES

1. M. Pollitt, E. Casey, D.O. Jaquet-Chiffelle, P.A. Gladyshev (2018): Framework for Harmonizing Forensic Science Practices and Digital/Multimedia Evidence Organization of Scientific Area Committees for Forensic Science, 10.29325/osac.ts.0002
2. M. Köhn, M.S. Olivier, J.H. Eloff (2006) July. Framework for a digital forensic investigation ISSA , pp. 1-7
3. E. Casey (2011) Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet Academic press, Amsterdam
4. A. Agarwal, M. Gupta, S. Gupta, S.C. Gupta (2011) Systematic digital forensic investigation model Int. J. Comput. Sci. Secur., 5 (1), pp. 118-131
5. F. Jafari, R.S. Satti (2015) Comparative analysis of digital forensic models. J. Adv. Comput. Netw., 3 (1), pp. 82-86, 10.7763/jacn.2015.v3.146
6. B.M. Staw (1981) The escalation of commitment to a course of action Acad. Manag. Rev., 6 (4) , pp. 577-587
7. M.D. Kohn, M.M. Eloff, J.H. Eloff (2013) Integrated digital forensic process model Comput. Secur., 38 (2013), pp. 103-115, 10.1016/j.cose.2013.05.001
8. X. Du, N.A. Le-Khac, M. Scanlon (2017) Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service arXiv preprint arXiv:1708.01730
9. Mustapha Saeed and Sone Osakwe, Researchers at the Centre for the Study of the Economies of Africa. https://www.linkedin.com/in/mustapha-sa-eed-59408a37
10. *Part 2: The Phase-oriented Advice and Review Structure (PARS) for digital forensic investigations*, Nina Sunde, Graeme Horsman