Exploring Digital Forensic Readiness: A Preliminary Study from a Law Enforcement Perspective

Odin Heitmann[1,2][0009−0002−3937−4715] and Katrin Franke[2][0000−0002−4899−9410]

[1] The National Criminal Investigation Service, Postboks 2094 Vika, 0125 Oslo, Norway
[2] Norwegian University of Science and Technology, Teknologivegen 22, 2815 Gjøvik, Norway
odin.heitmann@politiet.no

Abstract. In today's world of cybersecurity, it is not a question of *whether* an organization will experience a cyber attack, but rather a matter of *when* it will happen. These incidents can cause significant disruption and financial losses to organizations. Forensic readiness is becoming increasingly crucial as it can help maximize the use of digital evidence and reduce the investigative cost after an attack. It can also aid law enforcement in identifying and prosecuting cybercrime perpetrators. Our observation of cybercrime investigations indicates divergent stakeholder priorities during a cyber attack. Victimized organizations prioritize resuming normal operations, and incident responders focus on restoration, potentially neglecting criminal evidence integrity. Law enforcement involvement occurs post-incident, usually after the initial incident handling is completed. Due to divergent focus areas, there is a lack of a comprehensive overview. This made us question the relationship between forensic readiness practices in the industry and criminal investigations performed by law enforcement after an attack. This paper investigates whether forensic readiness and criminal investigation are aligned. To assess alignment, we compare forensic readiness and criminal investigation definitions and their core components. Our research shows that forensic readiness does not sufficiently focus on criminal investigation; thus, the current forensic readiness approach does not adequately encompass criminal investigations. We propose incorporating criminal investigation integration as a new domain to address this issue while developing future forensic readiness models and practices. Furthermore, we propose using the term cross-organizational investigative readiness instead of forensic readiness to underline the importance of the industry, incident responders, and law enforcement working together to prevent, mitigate, and prosecute cybercrime.

Keywords: Cybersecurity · Forensic readiness · Criminal investigation · Cross-organizational investigative readiness · Criminal Investigation Integration

1 Introduction

Cybercrime is a growing threat that organizations in both public and private sectors must be prepared to face, as it can have severe consequences. One instance of this occurred in 2019 when Norsk Hydro ASA fell victim to a major cyber attack [24]. Norsk Hydro is a leading manufacturer of aluminum and one of Norway's largest hydropower producers, with operations in over 50 countries, 34,000 employees, and a turnover of 159 billion NOK in 2018 [9]. The consequences of a successful cyber attack could be devastating, as was the case for Hydro. The cyber attack affected Hydro on a global scale, with the Extruded Solutions division facing the most operational challenges and financial losses. Furthermore, the estimated cost for Hydro in 2020 was around 800 MNOK [24]. The National Cybercrime Centre (NC3) in Norway is still investigating this crucial case four years after the attack. Although the Hydro criminal case is not yet concluded, it has revealed five males who are suspected of carrying out the actual attack, along with 56 other suspects. These suspects include individuals involved in money laundering, cryptocurrency activities, and providing various services [10]. The attacks by this group might have affected over 1800 victims in 71 countries [15].

Having admissible evidence is crucial for law enforcement to prosecute cybercrime cases such as the Hydro case in a court of law. The level of readiness of an organization's digital forensics can impact the identification and collection of potential digital evidence (PDE). Companies that lack proper readiness may not i) have the evidence due to them being lost during an attack, ii) be aware of their PDE, or iii) know how to access and collect it in a forensically sound manner. Companies operating in critical sectors add to the complexity of digital forensic evidence gathering, as their services must be provided 24/7, making it difficult to shut down operations for servers and data collection and acquisition.

Observing the Hydro criminal investigation from the sideline gave us valuable insights into the challenges with various stakeholders during a cyber attack. As illustrated in Fig. 1 on Page 3, various stakeholders' focus on different phases of cyber attacks and incidents. Organizations may prioritize cyber security hardening, the upkeep of their operations, and the return to a state of normalcy, as opposed to reactive measures such as investigating criminal incidents by law enforcement agencies (LEAs). Incident responders who first handle the disruption similarly strive to restore regular functioning. Although their efforts may reveal PDE that can assist LEAs, their primary focus may not involve maintaining the chain of custody or ensuring the integrity of evidence. LEAs often only get involved after an incident, which means they may not have been part of an organization's proactive preparedness plans or the implementation of measures for active incident plans, i.e., the organization's forensic readiness. This can result in LEAs being unaware of an organization's forensic capabilities, and organizations not knowing how they can collaborate with LEAs. This fragmented approach, with organizations and LEAs working in their own silos, may affect the quality and success of a criminal investigation. The results can be inadmissible evidence in court, and an increasing cost of the incident for the organization. A cross-

organizational investigative readiness could benefit organizations experiencing cyber attacks, law enforcement, and other stakeholders like national security at large.

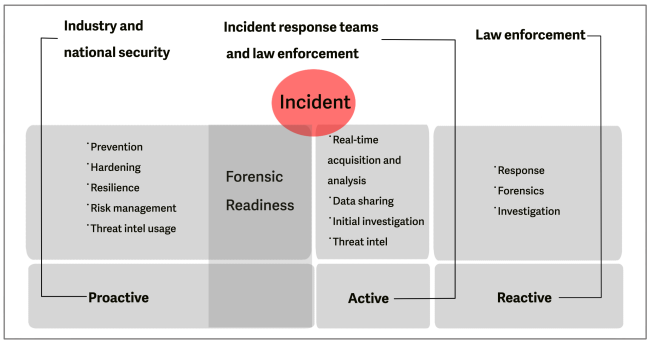

Fig. 1: Illustration based on a presentation by Franke on Forensic Readiness [16] shows how various stakeholders have different focus areas depending on the phase of an incident

In this paper, we present our research on the relationship between forensic readiness and criminal investigations to see if these practices are aligned or not. Our motivation was the realization that stakeholders have different focus areas, and a fragmented approach could affect the outcome of an investigation. We aim to establish a foundation for forensic readiness in the context of potential criminal investigations.

We used several approaches to explore the relationship between forensic readiness and criminal investigation. The first was data from a literature review we are currently working on; see Table 1 for applied methodology. The preliminary study for this paper focused only on forensic readiness and provided a strong indication of the current state of the art. After conducting the preliminary study on forensic readiness, we delved into the latest literature on cyber and criminal investigations in Norway and the definitions provided by Interpol and Europol to gain an understanding of the criminal investigation of cybercrime. Furthermore, we referred to relevant guidelines and standards frequently cited in the field.

The remainder of the paper is organized as follows: We start by presenting definitions and core components for forensic readiness, investigation, and socio-technical systems in Section 2. Next, in Section 3, we discuss the commonalities and incompatibility between forensic readiness and criminal investigation. In Section 4, we propose new components to be included in forensic readiness models, as well as a new term. Lastly, we conclude and suggest further research in Section 5.

Table 1: Applied methodology for literature review

Databases	IEEE Explore, Science Direct, ACM Digital Library, Springer Link, and Scopus
Search query	((Digital forensic readiness OR forensic readiness) AND ("critical infrastructure" OR "forensic ready system" OR "forensic ready software system" OR "forensic by design" OR "management system" OR "investigation" OR "cyber-physical" OR "SCADA" OR "IIOT" OR "DCS"))
Results	616 records, including 223 duplicates and 55 inaccessible records
Screening	338 records. Evaluation strategy: Must be relevant to forensic readiness in IT/OT systems in the critical sector
Full read	151 records. Exclusion criteria: Records not directly addressing forensic readiness or narrow scope (e.g. specific tooling)
Included	127 records. Preliminary study focused on forensic readiness

2 Definitions and core components

2.1 Forensic readiness

The term forensic readiness was initially coined by Tan in 2001 and was then described as the ability to maximize the usefulness of evidence data from incidents while minimizing the cost of forensics during an incident response [30]. The term has been refined and expanded by other researchers. In 2004, Rowlingson expanded forensic readiness to "*the ability of an organisation to maximise its potential to use digital evidence whilst minimising the costs of an investigation*", while describing forensic readiness as the knowledge that an incident will occur as well as the act of incident response [27]. This definition highlights digital evidence and investigation as a part of forensic readiness. In their work from 2010, Pangalos and Katos define forensic readiness as "*the state of the organisation where certain controls are in place in order to facilitate the digital forensic processes and to assist in the anticipation of unauthorised actions shown to be disruptive to planned operations*" [25]. In a comparative study conducted in 2018 by Park et al., a definition by CESG from 2015 is included, where forensic readiness is defined as *"the achievement of an appropriate level of capability by an organization in order for it to be able to collect, preserve, protect and analyze Digital Evidence so that this evidence can be effectively used in any legal matters, in disciplinary matters, in an employment tribunal or in a court of law"* [26,23]. Furthermore, Park et al. refer to "Guide to IT forensics" (Leitfaden IT Forensik) from 2011, where forensic readiness is differentiated between strategic readiness and operational readiness [26]. Park et al. also describe strategic readiness as preparing in advance, e.g., configuring servers for potential forensic investigations or providing an overview of data sources containing PDE, while operational readiness refers to the initial investigation, e.g., identifying PDE from various sources [26]. Notably, procedures from strategic readiness aim to support operational readiness. The common denominator for these definitions is how they describe forensic readiness as a capability, but they do not describe how an organization can achieve forensic readiness.

Researchers have proposed several approaches to achieving and continuously improving forensic readiness. Trcek et al. proposed a framework for forensic

readiness procedures differentiating on international, national, and organizational levels in 2010 [31]. In 2015, Elyas et al. proposed a refined framework where the forensic readiness capability of an organization hinges on organizational factors, a forensic strategy, forensic readiness objectives, and the relationships between the factors [11]. Grubor et al. proposed using multi-criteria decision-making methods to aid managers in improving forensic readiness in 2017 [17]. In 2022, Baiquni and Amiruddin conducted a case study of digital forensic readiness level measurement using a Digital Forensics Readiness Index proposed by Widodo in 2013 [7]. The indicators are based on several organizational components: Strategy, Policy and procedure, Technology and Security, Digital Forensic Response, Control, and Legality.

The importance for the organization to understand which structures, i.e., forensic readiness components or domains, are required before investing in forensic readiness resources is underlined by Bankole et al., and they argue the necessity for an assessment tool to measure forensic readiness maturity [8]. In their work from 2022, Bankole et al. propose the DFR Commonalities framework (DFRCFv2), which aims to aid organizations in implementing and managing forensic readiness programs. The framework is based on a set of domains, as illustrated in Fig. 2. The proposed domains are:

- *Strategy:* In addition to encouraging the implementation of forensic readiness throughout the organization, the strategy domain involves business goals and the organizational structure.
- *Legislation & Regulation:* This domain ensures that the organization's digital forensic readiness strategy considers all applicable laws and regulations for the organization.
- *Governance:* Governance involves managing the system, evidence, incident management, and best practices.
- *Compliance:* The compliance domain ensures adherence to policies and procedures. A report with findings is generated to indicate progress toward strategic goals and areas for improvement.
- *Training:* The training domain focuses on training strategies and awareness campaigns for digital forensics, aiming to foster forensic readiness and allow investigations to proceed at a proportional cost to the incident.
- *Systems & Events:* This domain involves identifying and classifying hardware, software, processes, and events within the organization that contain PDE. Additionally, it involves the organization's digital forensic capabilities.
- *Policy & Procedure:* Policies, procedures, technical standards, guidelines, and best practices for forensic readiness are all relevant to this domain.
- *Risk management:* Risk management, hereunder risk assessments, is a domain in itself.
- *Monitor & Report:* This domain relates to tools for monitoring, e.g., intrusion detection systems and requirements for monitoring. Conducting a cost/benefit analysis in this domain is also advisable before commencing an investigation. Some objectives of this domain are establishing consistent reporting procedures, creating an incident escalation policy, and providing guidelines for communication between relevant parties.

Fig. 2: Illustration of Digital forensic readiness commonalities v2 (DRFCFv2) domains, as proposed by Bankole et al. [8]

The DRFCFv2 framework has similarities with a socio-technical system model approach. To better understand how these frameworks are constructed, we have provided socio-technical system model fundamentals in Section 2.3.

To support the definition and implementation of forensic readiness, international standards like ISO/IEC can be used. ISO/IEC 27043 is a standard related to incident investigation principles and processes, and while not clearly stated, it expands on the aim of forensic readiness by Tan presented earlier in this section, to also minimize interference and prevent interruption of an organization's business processes, in addition to the preservation and improvement of the current level of information security of systems within the organization [19]. The standard provides an overview of activities that can be conducted based on readiness processes for planning, implementation, and assessment, e.g., identification and implementation of pre-incident gathering of PDE. Section 9.3 in ISO/IEC 27043 states the following: *"Potential digital evidence must be collected in such a manner that its integrity is preserved. This is important if one needs to use this evidence at a later stage to draw some formal conclusions, i.e. in a court of law. Adhering to strict legal regulations during the evidence collection process is of crucial importance, as digital evidence might become unusable when proper procedures are not followed"*. This underscores the importance of preserving PDE integrity for forensic analysis and legal proceedings.

2.2 Investigation and criminal investigation

Uncovering important details regarding a crime or incident using a systematical approach is one of an investigation's key objectives [6]. The *5WH* formula can aid investigators in determining the answers to the following questions: what happened, when did it happen, where did it happen, who was involved, why did it occur, and how did it happen

The term *investigation* refers to a systematic and comprehensive process of gathering, analyzing, and evaluating information, evidence, and facts to uncover and understand the details surrounding a particular event, situation, or circumstance. It involves a methodical approach to discover truths, identify potential causes, and reach conclusions based on available data and resources. To structure the investigation, the questions from the 5WH formula can be used (Who - Where - What - When - Why - How) [4,5,28,19]. Alenzi et al. argue that summarizing the investigation results using a 5WH formula and following forensic techniques can support the collection of PDE, which then can be used in a

court of law [3]. A 5WH formula to aid cybercrime investigations with relevant questions was proposed by Sunde in 2023 [29], as shown in Fig. 3.

The difference between an investigation as described above and a *criminal* investigation is who performs the investigation and what the end goal is. An investigation can be conducted within an organization, with or without suspicion of criminal activity. For instance, an investigation can be carried out to identify the underlying cause of suboptimal performance and to find ways to improve the situation. On the other side, a criminal investigation is carried out[3] when, as a result of a report or other circumstances, there is *reasonable reason* to investigate whether there is a criminal offense being pursued by the public authorities [1]. The purpose of a criminal investigation is to gather necessary information for four main reasons [2], which are to:

a) decide the issue of indictment
b) serve as a preparation for the court's consideration of the question of criminal guilt and, if applicable, the question of determining a legal consequence
c) prevent and stop criminal activity
d) carry out punishment and other reactions

To better understand criminal investigations of cybercrime criminal cases, there is a need for a definition of *cybercrime*. Interpol uses a distinction between *cyber-dependant* crimes and *cyber-enabled* crimes from The United Kingdom Home Office [20]. The United Kingdom Home Office defines cyber-dependant crimes as offenses that rely on a computer, computer networks, or other information communications technologies (ICT), while cyber-enabled crimes are traditional crimes that are increased in scale or reach by utilizing computers, computer networks, or ICT [22]. Criminal cases involving ransomware and hacking will be labeled cyber-dependant crimes. Europol uses the term *High-Tech Crime* to describe a form of cybercrime that uses electronic and digitally based technology to attack computers or a computer network [14]. Whenever we use the term cybercrime in this article, we refer to the definition of High-Tech Crime used by Europol for simplicity.

When investigating criminal cases related to cybercrime, there are two main components to consider; traditional criminal investigation and the digital forensics process. Sunde argues the necessity of having knowledge in various areas, including methodology, law, and technology, to investigate cybercrime effectively [29]. In 2023, Sunde also proposed an integrated framework for cyber investigations (ICIP) to help everyone involved in these investigations have a shared understanding of the overall goal [29]. The framework builds upon earlier work by Hunton (2003), Innes (2007), and Fahsing (2016) and aims to *"integrate the components of criminal investigation and technology examination"*. The ICIP describes a non-linear, cyclic process that can be followed until the investigation is completed, i.e., when the purpose of the investigation is fulfilled. Even though it is non-linear, the author underlines that skipping stages is impossible, exemplified by going from initial investigation to action, which would be erroneous.

[3] The prerequisites for starting a criminal investigation and the objective of such investigation may vary between countries.

The ICIP, as illustrated in Fig. 4, includes core principles (CP) and process components (PC) [29]:

- *(CP) Legality:* The ICIP assumes that criminal procedural rules that apply to the relevant area are followed, in addition to applicable ethical guidelines and in accordance with basic human rights.
- *(CP) Forming and testing of hypotheses:* Extensive use of hypothesis thinking is central to the ICIP model. A distinction is made between three levels of the hypotheses. The offense level describes objective elements, exemplified by the fact that someone has hacked a company's network and stolen confidential information. The activity level describes actions carried out, regardless of whether the action is criminal activity or not, exemplified by the fact that malware was sent from e-mail alice@mail.com to e-mail bob@mail.com. The source level describes the source of identified traces, e.g., that suspect Alice used the email address alice@mail.com when she sent the malware.
- *(CP) Digital evidence handling:* Maintaining the integrity of digital evidence is of utmost importance. Any deviation from this protocol must be properly documented and justified to ensure the credibility of the evidence. An audit trail and documentation of the chain of custody for the digital evidence should also be present.
- *(PC) Investigation initiation:* One of the key tasks in this component is to obtain an overview, identify an initial investigative hypothesis at the offense level, and plan the initial actions for collecting relevant information.
- (PC) Modeling: All relevant information must be promptly gathered and organized in this stage, and all potential offense-level investigative theories should be established.
- *(PC) Impact and risk assessment:* Before proceeding with any planned actions, reviewing and crosschecking them against the relevant legislation and policy is essential. Identifying potential risks and taking measures to minimize them is also crucial. Additionally, it is important to consider the impact of handling PDE, as it may contain traces of DNA and fingerprints that can be destroyed or contaminated if not handled correctly.
- *(PC) Action and collection:* This involves gaining control and an overview of the search scene, specifically the area where PDE may be located. The order of collection and acquisition of PDE should be prioritized, and PDE should be collected using a forensically sound methodology.
- *(PC) Analysis and integration:* The aim of this stage is to identify relevant information that can be used to test investigative hypotheses. This establishes the credibility of the information using a structured and transparent approach.
- *(PC) Documentation and presentation:* When presenting information gathered during an investigation, it is important to consider the intended audience and present the information in a clear and understandable format using appropriate language. Any uncertainty surrounding the information should also be disclosed, and a distinction should be made between factual findings and opinions.
- *(PC) Evaluation:* One way to assess the success of an investigation and identify areas for improvement is through an evaluation stage. This can also help to prevent future errors and promote effective and efficient practices.

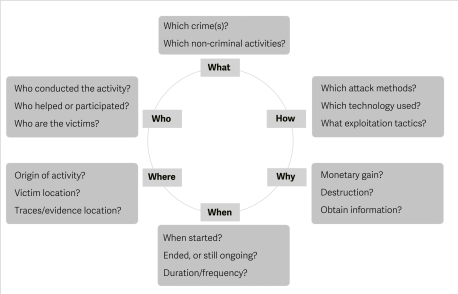

Fig. 3: Illustration of The cyber investigation queries, by Sunde [29]

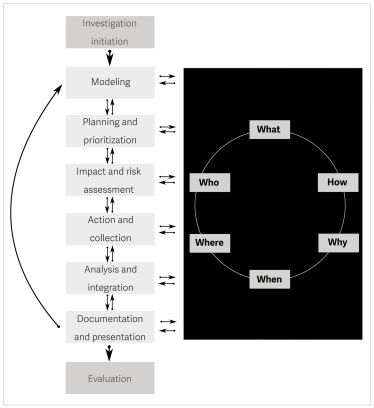

Fig. 4: Illustration of The Integrated Cyber Investigation Process (ICIP), by Sunde [29]

2.3 Socio-technical systems

A socio-technical approach is useful to analyze the connection between technology and human (social) factors needed for forensic readiness, especially from a law enforcement and criminal investigation viewpoint. Linstone's approach, as cited in Kowalski [21], can be utilized as a thinking tool to offer insights into system behavior and detect potential leads. By creating a socio-technical system model, we can better understand the interdependence between technical and social aspects.

The components in a socio-technical system strive for balance, and Kowalski calls it socio-technical insecurity if the system cannot reach balance after an internal or external disturbance [21]. In an organizational context, the organization itself can be a socio-technical system. Using Hydro as an example, the Hydro organization was a socio-technical system striving for balance - and most likely a rather balanced system - before the ransomware attack in 2019. The ransomware attack was a huge external disturbance that forced Hydro's socio-technical system to implement actions to restore the balance.

Some existing forensic readiness models use components that can be used in a socio-technical system model. The DFRCFv2, as presented in Section 2.1, has domains that are transferrable into a socio-technical system model. The strategy and governance domains relate to the organizational structure and management of systems, and thus, it can be argued to relate to *Social - Structure*. The training domain seeks to influence the *Social - Culture*, while the domains Systems & Events and Monitor & Report relate to *Technical - Machines*. Finally, the domain Policy & Procedure involves best practice, which makes it relatable to *Technical - Methods*. A simplified version of a socio-technical system, with the potential placement of forensic readiness components, is illustrated in Fig. 5. The research conducted by Elyas et al. in 2014 and 2015 examines the various

factors within an organization that contribute to forensic readiness [12,11]. Their work also explores how these factors work together to achieve the desired outcome. Although their research is not based on a socio-technical system model, it provides a clear and transparent approach to identifying the interconnected components necessary for building forensic readiness, which could be used in a socio-technical system model for forensic readiness.

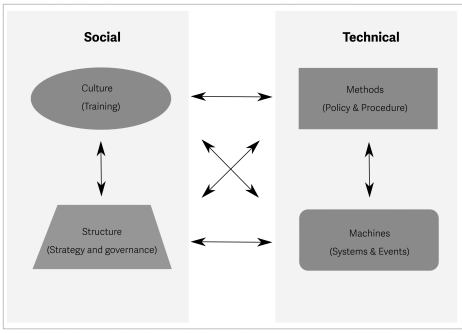

Fig. 5: A Socio-technical System, based on Kowalski [21], with an example of forensic readiness components

3 Discussion

This section will discuss where forensic readiness and criminal investigation objectives and components are aligned and where we believe they differ. We will first discuss the aligned parts before we discuss where they differ.

3.1 Forensic readiness and criminal investigation commonalities

Legality: One important forensic readiness component is legality. Having a legal foundation and backing is required to do various tasks. To acquire PDE by copying, it needs to be legal for the organization. Similarly, almost all actions taken by law enforcement have to be founded on a law, and the ICIP has legality assessment as one component.

Risk assessment: As seen in the DFRCFv2, risk management is a domain by itself, with only risk assessment as a sub-domain. This makes it clear that risk assessment is necessary to achieve forensic readiness. Criminal investigations also do risk assessment by focusing on identifying potential risks and taking measures to minimize them. However, risk assessment for an organization will differ and have many more facets than cybercrime investigations, where the focus is risks related to PDE.

Collection of PDE: The concept of forensic readiness is to ensure best practices are followed to maintain the integrity of digital evidence. The same level of focus is observed in the ICIP. However, the level of integrity required may differ between forensic readiness and criminal investigations. Law enforcement needs to present the digital evidence to a court of law, thus requiring a higher degree of integrity. Forensic readiness practices do not require an absolute level of integrity to be maintained, with the result that maintaining integrity for evidential purposes during incident response is hardly practiced.

Reporting and presentation: The results from forensic readiness and CI will end up in a report where the content is tailored for the intended audience. The main difference is that the report from a criminal investigation is mainly intended for a court of law, while the audience for forensic readiness reports is a variety of stakeholders depending on the purpose of the internal investigation.

Evaluation: Both forensic readiness and criminal investigations focus on improving through evaluation. Forensic readiness uses governance to learn from past events, while criminal investigations evaluate and improve investigative procedures.

3.2 Forensic readiness and criminal investigation misalignment

Handling of PDE: Forensic readiness focuses on keeping the integrity of PDE intact, but it is not an absolute requirement. Therefore, even though organizations have implemented forensic readiness, they do not have strict requirements for handling PDE during an incident, and it is not guaranteed the PDE they have collected is treated in a way that makes the PDE admissible in a court of law. This might be problematic if an incident at a later stage is escalated to a criminal investigation, and the initial handling of PDE was not following strict guidelines. On the other side, law enforcement is bound by laws, and they will therefore strive to acquire *all* PDE in a manner that makes it admissible in a court of law from the beginning. As presented in Section 2.1, ISO/IEC 27043 states that the integrity of PDE collected must be maintained *"if one needs to use this evidence at a later stage to draw som formal conclusions, i.e., in a court of law"*. We believe the real concern lies in cases that begin as minor incidents and then escalate into major ones and even criminal investigations. It is important to follow strict procedures from the start to ensure the integrity of potential digital evidence. Failure to do so can render the use of PDE inadmissible in a court of law.

Ownership of an attack: At times, it can be difficult to identify whether a cyber incident is a cybersecurity issue affecting corporate or national infrastructure, a cybercrime where an actual crime is being committed, or a combination of the two. In case it is established that the incident is a cybercrime, law enforcement must take immediate action. In case of a cybersecurity incident, external incident responders such as a Computer Emergency Response Team (CERT) or a Computer Security Incident Response Team (CSIRT) usually take charge [14]. However, distinguishing between cyber incidents and cybercrime during the

initial phase can be tricky. As a result, we suggest that all necessary stakeholders are involved from the outset of an incident that affects high societal value organizations or organizations related to critical infrastructure. This will ensure a coordinated and efficient response.

Planning to escalate from incident to criminal investigation: Forensic readiness focuses on preparing for an incident and how to handle an incident, and therefore, proactive planning is a natural part of forensic readiness. On the other hand, law enforcement is traditionally reactive, and their investigation does normally not start *before* a crime has been committed. We believe that forensic readiness lacks the criminal investigation aspect when handling PDE. The approach can vary depending on the outcome, which is almost impossible to determine before answering the incident's five W's and one H (5WH).

Cooperation between organizations and law enforcement: As presented in Section 2.1, several authors define forensic readiness as something that has to do with digital evidence and the evidentiary value to be used in a court of law. This implies that law enforcement could benefit from being part of an organization's forensic readiness capability, especially considering that an investigation can be escalated to a criminal investigation. However, law enforcement is normally first involved in the forensic process when a crime has been committed or when the crime has been discovered and reported [18]. Being used to handling evidence using proper methods to maintain integrity so the evidence can be presented in a court of law, law enforcement digital forensic specialists are familiar with the proper requirements. This means that external parties such as incident responders need to understand how to handle PDE to maintain its integrity at the same level as law enforcement specialists. The consequence, if the first responder is not properly trained in the handling of PDE, is, as pointed out by Hoolachan and Glisson, that vital evidence can be lost or altered in a way that makes it inadmissible in court and therefore hinder a prosecution [18]. Rowlingson also points out that *"a major criminal incident may involve the police"*, and prior preparations between organizations, incident responders and law enforcement can therefore enhance the coordination during such incidents [27].

4 Integrating Criminal Investigation and Defining Cross-organizational Investigative Readiness

Based on our initial study of both the commonalities and incompatibilities between forensic readiness and criminal investigation, we argue that there are several misalignments that could be remedied by incorporating a new component into future forensic readiness models and practices. We also argue that the term forensic readiness is insufficient to describe the cross-organizational preparation and capability needed to prevent, mitigate, and prosecute cybercrime. In this section, we argue that criminal investigation needs to be integrated into forensic readiness models and practices. To foster clear communication and mutual understanding between organizations, we propose the term cross-organizational investigative readiness to encompass forensic readiness's investigative aspect.

4.1 Criminal Investigation Integration

Policy, technology, and people are crucial elements to achieve forensic readiness, as shown in related work; see Section 2.1. Unfortunately, existing forensic readiness models do not embrace the importance of criminal investigation needs by law enforcement, and we believe this to be a weakness for an incident response that might evolve into a criminal investigation. To reduce the gap between forensic readiness and criminal investigation of cybercrime, we propose to build on the DFR Commonalities framework (DFRCFv2) by Bankole et al. [8], incorporating **Criminal Investigation Integration** as a new domain for ensuring criminal investigation needs in forensic readiness models and practices, as shown in Fig. 6 below.

Fig. 6: DFRCFv2 with criminal investigation integration as a new domain

The use of a socio-technical system model approach can help to visualize the dependencies within the forensic readiness domain, making it easier for organizations and LEAs to adopt the forensic readiness approach, while also incorporating the criminal investigative perspective. By including criminal investigation into an organization's forensic readiness capability, it becomes a constant overlay, serving as a known entity. Fig. 7 illustrates the criminal investigation integration overlay, using the simplified socio-technical system model presented in section 2.3.

Employing a socio-technical system model approach can improve the transparency of dependencies within the forensic readiness domain. This, in turn, streamlines the adoption of the forensic readiness approach by organizations and law enforcement, all while facilitating the integration of investigative readiness.

4.2 Cross-organizational Investigative Readiness

The realization that it's not a matter of *if* you'll experience a cyber attack or breach, but *when*, is not new, and in 2004, Endicott-Popovsky and Frincke added a fourth strategy to the existing strategies from the CERT's 3R model for survivable systems [13]. The fourth strategy was *redress*; the ability to hold intruders accountable in a court of law and the ability to retaliate. From a law enforcement perspective, this indicates that the desire is not only to repel attacks or quickly recover but is accompanied by a need to see justice served for the criminals behind the attacks.

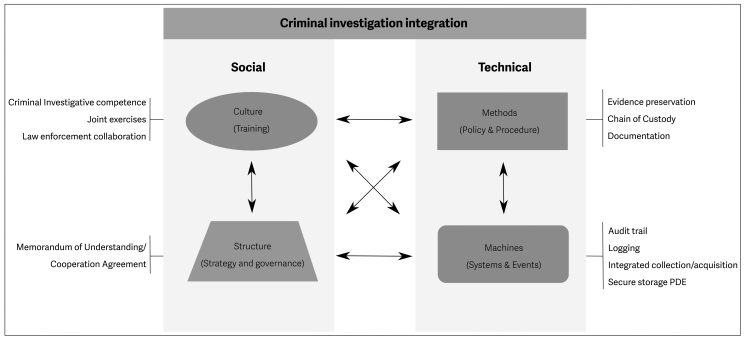

Fig. 7: A socio-technical system, based on [21], with criminal investigation integration as an overlay

To signify that the ability to redress is crucial to prevent, mitigate, and prosecute cybercrime, we do not believe the term forensic readiness is sufficient, as this term does not encompass an investigative capability suited for criminal investigation. Neither does this term emphasize the importance of involving law enforcement in forensic readiness capability building and maintenance phases. Thus, we propose the following term:

Cross-organizational Investigative Readiness. *An intentional preparedness, agreed upon across relevant stakeholders, for potential forensic criminal investigation and collaboration in the future, where the applied methodology and handling of potential digital evidence will be conducted in a manner so that the potential digital evidence is usable for both incident response but also in a manner that ensures it can be used for criminal investigations, prosecutions and ultimately in a court of law.*

5 Conclusion and future research

Our research aimed to investigate the connection between forensic readiness and criminal investigations. We found that current forensic readiness practices do not sufficiently address criminal investigations. We believe it is crucial to incorporate criminal investigation into forensic readiness to ensure that potential digital evidence is admissible in court from the beginning of an incident. This is especially important for critical infrastructure and other high-profile organizations, which should follow strict guidelines for handling potential digital evidence. Failure to handle potential digital evidence correctly may lead to it being inadmissible in court, complicating the investigation and potentially allowing perpetrators to escape justice.

Unprepared organizations can face negative consequences due to law enforcement involvement during a criminal investigation, leading to unnecessary tension and hindering collaboration. We suggest introducing criminal investigation integration as a new component of future forensic readiness models to address this

issue. We also propose the term cross-organizational investigative readiness to describe the preparedness and collaboration needed between relevant organizations to ensure the methodology used and handling of potential evidence makes it admissible in court.

This research is exploratory and does not encompass all components of forensic readiness and criminal investigation concerning cybercrimes. Its objective is to lay the groundwork for comprehending the correlation between criminal investigation and forensic readiness, which can be further developed in subsequent studies. This research focuses mainly on Norwegian laws, but it is crucial to acknowledge that laws in other nations, and even global laws, may vary. Upcoming studies could focus on adopting and further expanding forensic readiness models and practices and evolving them into cross-organizational investigative readiness models and practices.

Acknowledgements This research was funded, in whole or in part, by The Research Council of Norway [338691]. For the purpose of open access, the author has applied a CC BY public copyright license to any Author Accepted Manuscript (AAM) version arising from this submission.

References

1. Act relating to legal procedure in criminal cases [The Criminal Procedure Act]. Lov om rettergangsmåten i straffesaker [Straffeprosessloven]. Chapter 18, Section 224. Norway. (2022)
2. Act relating to legal procedure in criminal cases [The Criminal Procedure Act]. Lov om rettergangsmåten i straffesaker [Straffeprosessloven]. Chapter 18, Section 226. Norway. (2022)
3. Alenezi, A., Atlam, H.F., Wills, G.B.: Experts reviews of a cloud forensic readiness framework for organizations **8**(1), 11. https://doi.org/10.1186/s13677-019-0133-z, https://doi.org/10.1186/s13677-019-0133-z
4. Årnes, A.: Digital forensics. John Wiley & Sons (2017)
5. Årnes, A.: Cyber Investigations. John Wiley & Sons (2023)
6. Årnes, A.: Introduction. In: Årnes, A. (ed.) Cyber Investigations, pp. 1–12. John Wiley & Sons (2023)
7. Baiquni, I., Amiruddin, A.: A case study of digital forensic readiness level measurement using DiFRI model. pp. 184–189. https://doi.org/10.1109/ICIMCIS56303.2022.10017686
8. Bankole, F., Taiwo, A., Claims, I.: An extended digital forensic readiness and maturity model **40**, 301348. https://doi.org/10.1016/j.fsidi.2022.301348
9. Bryhn, R., Gram, T.: Norsk Hydro (2023), https://snl.no/Norsk_Hydro, *Accessed August 20th, 2023*
10. E24: Kripos mener å ha oppklart løsepenge-angrepet mot Hydro (2023), https://e24.no/naeringsliv/i/EQ5m6K/kripos-mener-aa-ha-oppklart-loesepenge-angrepet-mot-hydro, *Accessed August 20th, 2023*
11. Elyas, M., Ahmad, A., Maynard, S., Lonie, A.: Digital forensic readiness: Expert perspectives on a theoretical framework **52**, 70–89. https://doi.org/10.1016/j.cose.2015.04.003

12. Elyas, M., Maynard, S., Ahmad, A., Lonie, A.: Towards a systemic framework for digital forensic readiness **54**(3), 97–105. https://doi.org/10.1080/08874417.2014.11645708
13. Endicott-Popovsky, B., Frincke, D.: Adding the fourth "R" [CERT's model for computer security strategies]. In: Proceedings from the Fifth Annual IEEE SMC Information Assurance Workshop, 2004. pp. 442–443. IEEE (2004)
14. Europol: High-Tech Crime (2022), https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/cybercrime/high-tech-crime, *Accessed August 28, 2023*
15. Europol: 12 targeted for involvement in ransomware attacks against critical infrastructure (2023), https://www.europol.europa.eu/media-press/newsroom/news/12-targeted-for-involvement-in-ransomware-attacks-against-critical-infrastructure, *Accessed September 5th, 2023*
16. Franke, K.: Presentation at Dagstuhl Seminar (February 2014)
17. Grubor, G., Barac, I., Simeunovic, N., Ristic, N.: Achieving business excellence by optimizing corporate forensic readiness **19**(44), 197–214
18. Hoolachan, S.A., Glisson, W.B.: Organizational handling of digital evidence (2010)
19. International Organization for Standardization: Information technology — security techniques — incident investigation principles and processes. ISO Standard ISO 27043, ISO (2015), https://www.iso.org/standard/44407.html
20. Interpol: National Cybercrime Strategy Guidebook (2021), https://www.interpol.int/content/download/16455/file/Cyber_Strategy_Guidebook.pdf, *Accessed August 28th, 2023*
21. Kowalski, S.: It insecurity: A multi-disciplinary inquiry. (1996)
22. McGuire, M., Dowling, S.: Cyber crime: A review of the evidence. Summary of key findings and implications. Home Office Research Report 75 (2013), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf, *Accessed September 7, 2023*
23. National Technical Authority For Information Assurance: Good Practice Guide Forensic Readiness **1.2** (2015)
24. Norsk Hydro ASA: Cyber-attack on Hydro (2020), https://www.hydro.com/en-NO/media/on-the-agenda/cyber-attack/, *Accessed August 20th, 2023*
25. Pangalos, G., Katos, V.: Information assurance and forensic readiness. In: Next Generation Society. Technological and Legal Issues: Third International Conference, e-Democracy 2009, Athens, Greece, September 23-25, 2009, Revised Selected Papers 3. pp. 181–188. Springer (2010)
26. Park, S., Akatyev, N., Jang, Y., Hwang, J., Kim, D., Yu, W., Shin, H., Han, C., Kim, J.: A comparative study on data protection legislations and government standards to implement digital forensic readiness as mandatory requirement **24**, S93–S100 (2018). https://doi.org/10.1016/j.diin.2018.01.012
27. Rowlingson, R.: A ten step process for forensic readiness. International Journal of Digital Evidence **2**(3), 1–28 (2004)
28. Stelfox, P.: Criminal investigation: An introduction to principles and practice. Routledge (2013)
29. Sunde, N.: Cyber investigation process. In: Årnes, A. (ed.) Cyber Investigations, pp. 13–50. John Wiley & Sons (2023)
30. Tan, J.: Forensic readiness. Cambridge, MA:@ Stake **1** (2001)
31. Trček, D., Abie, H., Skomedal, A., Starc, I.: Advanced framework for digital forensic technologies and procedures **55**(6), 1471–1480. https://doi.org/10.1111/j.1556-4029.2010.01528.x