Research on digital investigation procedures for computer network security monitoring of the Quang Ninh Provincial People's Committee

Dinh Thi Thuy Huong

Abstract: This study develops a digital investigation process tailored to the cybersecurity monitoring needs of the Quang Ninh Provincial People's Committee. Recognizing the increasing sophistication of cyber threats targeting local government networks, the research addresses the gap between generic digital forensics frameworks and the specific operational, legal, and administrative constraints of a provincial administrative body. Through a combination of literature review, analysis of existing incident response protocols, and practical evaluation of current monitoring infrastructure, the study proposes a structured, multi-phase procedure. The process encompasses pre-incident preparation, secure evidence acquisition, chain-of-custody management, forensic analysis, and reporting, all aligned with Vietnamese legal standards and the committee's organizational hierarchy. Key features include integration with existing Security Operations Center (SOC) tools, role-specific responsibilities for IT staff, and protocols for handling sensitive administrative data. The findings offer a replicable model for enhancing proactive threat detection and post-incident accountability, ultimately strengthening the cybersecurity resilience of local government digital ecosystems.

Keywords: Digital forensics, network security monitoring, investigation procedures, provincial government