THE ROLE OF TECHNICAL EXPERTISE IN CYBERCRIMES

[1]ALI SAIF ALQAYDI, [2]MAHER ALJABER

[1]Master of Cybersecurity Law, Fujairah University
[2]Associate Professor of Cybersecurity Law, Faculty of Law. Fujairah University
E-mail: [1]202510354@fu.ac.ae, [2]m.aljaber@fu.ac.ae, maheraljaber@bau.edu.jo

Abstract - The world has witnessed in recent decades a tremendous technological revolution that has impacted various aspects of life, driven by the widespread expansion of the internet and modern communication technologies. This development has led to the emergence of new forms of crime known as cybercrimes. These crimes are committed using information systems, networks, or smart devices, posing a significant challenge for judicial and security authorities compared to traditional crimes due to the difficulty of detecting and proving them. This study focuses on examining the role of technical expertise in cybercrimes by highlighting its importance in collecting and analyzing digital evidence. The study adopts a descriptive-analytical approach, which involves analyzing legal texts and relevant jurisprudential studies related to the research topic. The study has reached several key findings, most notably that technical expertise is one of the most important means of proof in the context of cybercrimes. This necessitates maintaining the integrity of procedures for collecting and preserving digital evidence. The study also offers several recommendations, the most important of which is the need to adopt unified standards for the work of technical experts to ensure the accuracy, quality, and reliability of the reports submitted before the judiciary.

Keywords - Cybercrime, Technical Experience, Technical Expert, Digital Evidence

I. INTRODUCTION

In recent decades, the world has witnessed a tremendous technological revolution whose effects have extended to various aspects of life. The widespread use of the internet in cyberspace has led to the emergence of new forms of crime known as cybercrimes. These are considered a new type of crime committed using information systems, networks, or smart devices.

This emerging type of crime has become a major challenge for courts and security agencies in different countries due to its unconventional nature, particularly the difficulty of detecting and proving such crimes. The process of proof in cybercrimes differs significantly from that in traditional crimes. While traditional crimes rely on physical evidence to establish proof, such evidence is often absent in cybercrimes. Instead, the evidence presented is intangible, requiring advanced technical and technological tools to handle digital evidence. This highlights the crucial role of technical expertise in uncovering such crimes and analyzing the evidence collected.

1.1. The Problem of the Study

The research problem revolves the determining the effectiveness of technical expertise in detecting and proving cybercrimes by clarifying the concept of technical expertise within the scope of cybercrime, the importance of the technical expert's role in collecting and analyzing digital evidence, and the extent to which the technical expert's opinion in the technical report they submit is binding on the judge's ruling in the case.

1.2 The Methodology

This study based on the descriptive-analytical method, which involves examining the legal texts relevant to the subject, along with analyzing the opinions of legal scholars and previous literature that have explored the role of technical expertise in cybercrimes. The study will first address the concept of technical expertise in the first section, followed by an identification of the role of technical expertise in cybercrime in the second section.

1.3 The Importance of the Study

The significance of this study lies in the fact that cybercrime is considered one of the most serious challenges facing societies today, in light of rapid digital advancement. These crimes leave profound impacts on economic, security, and social levels. Accordingly, the importance of technical expertise emerges in detecting such crimes, contributing to strengthening the legal value of expert reports and clarifying their effect on shaping the judge's conviction and the ruling issued in the case.

II. THE NATURE OF TECHNICAL EXPERIENCE

Experience is considered one of the fundamental concepts in various scientific and practical fields. It generally refers to the skills and knowledge that an individual acquires in a specific area as a result of practical practice, specialized study, or both. It is not merely theoretical knowledge, but rather the outcome of continuous interaction between learning and application, which gives a person a distinctive ability to understand, analyze, and deal with problems effectively. Therefore, a person who possesses these skills is referred to as an "expert," due to their

distinction in their field and their ability to provide a technical or scientific opinion based on precise foundations (Alghafri, 2015).

Expertise is characterized by combining both the theoretical and practical aspects. Academic training alone is not sufficient to acquire the status of an expert; it must be reinforced by practice and extensive hands-on experience. True expertise develops through the accumulation of knowledge and continuous experience, which gives the expert the ability to analyze accurately and make sound decisions. Therefore, expertise is considered a crucial element in many fields, especially in criminal investigations and informatics, where it contributes to uncovering facts and reaching precise results that serve justice (Hudood & Ahmad, 2025).

Technical expertise can be defined as a means of criminal proof employed to assist the judge or public prosecutor in technical matters that would be difficult for them to grasp without the help of specialists. Thus, technical expertise enables the judge to understand all the facts related to the disputed case by clarifying the technical aspects. A cybercrime expert is a scientifically and practically qualified person in the field of information technology and digital evidence analysis. They are commissioned by the competent authorities to examine electronic media and extract data related to the crime. The appointed expert works to uncover the mechanism of the crime by tracing the perpetrator through examining Internet Protocol (IP) addresses and interpreting the obtained digital evidence, which is often encrypted and can only be deciphered by the expert (Hudood & Ahmad, 2025).

The UAE legislator has recognized the importance of technical expertise in cybercrime cases. The UAE legislator, in Federal Decree-Law No. 34 of 2021 regarding rumors and cybercrimes, emphasized the role of the technical expert in such crimes by acknowledging the evidentiary value of digital evidence, provided that it is collected and preserved in accordance with legal and technical requirements. This indirectly highlights the role of the technical expert in collecting, analyzing, and interpreting the evidence that has been gathered.

III. THE IMPORTANCE OF TECHNICAL EXPERIENCE IN THE JUDICIARY

The importance of technical expertise in the judiciary is evident in its effectiveness in assisting judges to understand technical matters that fall outside their legal knowledge, particularly in interpreting and accurately explaining digital evidence in a way that aligns with reality. This expertise contributes to enhancing the accuracy of judicial rulings through the expert opinions provided by specialists. Therefore, technical expertise plays a significant role in supporting and strengthening the judge's ability to form their judicial convictions, especially in cases based on purely technical evidence. Ultimately, it helps bridge the gap between law and technology within the courtroom and strengthens the guarantees of achieving justice in emerging cybercrime cases (Hudood & Ahmad, 2025).

The importance of expert evidence lies in its contribution to the evaluation of evidence rather than merely presenting it. It is not considered an independent form of evidence in itself, but rather a technical analysis of existing evidence that assists the judge in assessing its legal value. Through this role, expert evidence helps enhance the accuracy of judicial rulings and reduce the likelihood of error, as it bridges factual data and scientific knowledge, thereby supporting the attainment of a sound judicial conviction.

Furthermore, the importance of expertise also lies in supporting investigation procedures and facilitating the work of judicial authorities, as it enables the uncovering of hidden aspects of cases, especially in specialized fields such as cybercrime. Experts possess skills and techniques that allow them to analyze evidence and draw conclusions that a judge or investigator may find difficult to reach on their own. This makes expertise a complementary and essential element in achieving justice and uncovering the truth.

Therefore, the UAE legislator, in the Federal Decree-Law No. 34 of 2021 relevant the Combating Rumors and Cybercrime, has affirmed the probative value of digital evidence, provided that it is obtained in accordance with proper legal procedures. This underscores the role of the technical expert through the expert report that he submits before the court or the Public Prosecution. If the judge has doubts regarding the expert report, then, pursuant to the powers granted to him under the Law of Evidence and related legislation, he may request that the expert submit another report or even appoint a different expert to provide an alternative report, in order to ensure impartiality and verify the accuracy of the results presented in the expert report.

One of the most important features that distinguishes expert evidence from other means of proof, such as investigation, testimony, and search, is the presence of a technical opinion provided by a specialized expert. This expert personally works on uncovering the indications found in the digital evidence and determining its evidentiary value. This is something the judge himself cannot establish, due to the presence of technical aspects in the evidence that he is unaware of and cannot understand except by seeking the assistance of a specialist.

The work of a technical expert is crucial in the field of cybercrime detection. The expert's role may focus on monitoring websites that constitute a crime in themselves, such as those involved in threats, defamation, copyright infringement, or even the dissemination of obscene images intended to promote prostitution and human trafficking. The expert's role may also extend to monitoring websites whose

content does not inherently constitute a crime, but which allow the expert to track individuals committing crimes. This includes websites that facilitate the identification of drug dosages or even those that visit websites to learn about drug cultivation or bomb-making techniques (Al-Zoubi & Al-Manasah, 2010).

In order to reach those crimes and pursue their perpetrators, the expert's role involves attempting to uncover digital evidence and identify its unique characteristics, and creating an original copy of the digital evidence to ensure that no information is missing during its collection. The expert also works on preserving the digital evidence to prove that it is authentic and reliable. To achieve this, the expert uses several tools that assist in their task, including Internet Protocol (IP) addresses, proxies (PROXY), tracking software, and intrusion detection systems (Tabri, 2020).

IV. CONCLUSION

The current study yielded several findings, including:

1. Technical expertise is considered one of the most important means of proof in the context of cybercrimes, due to the complex technical nature of this type of crime. The technical expert plays a pivotal role in analyzing and interpreting digital evidence in a way that facilitates the judge's understanding of the facts in dispute presented before him.
2. Technical expert reports in cybercrime cases are of great importance in understanding the case presented before the judge; however, the judge has discretionary authority to accept or reject the submitted report, pursuant to the powers granted to him under the law.
3. There is a close correlation between the competence of the technical expert and its impact on the accuracy and effectiveness of the evidentiary process in electronic cases.

In the light of the findings and the accelerating pace of digital transformation, the study concluded with several recommendations, summarized as follows:

1. The necessity of adopting standardized criteria for the work of technical experts in order to ensure the quality, neutrality, and accuracy of reports submitted to the judiciary.
2. The need to strengthen international cooperation in the field of combating cybercrime and to exchange technical expertise and information between countries.
3. The necessity of training judges in technical knowledge that helps them understand the technical reports submitted to them.

REFERENCES

[1] Alghafri, H. 2015. Criminal Policy in Confronting Internet Crimes. Al Obeikan Publishing.

[2] Al-Zoubi, J., and Al-Manasah, O. (2010).Technological Crimes of Electronic Information. Systems, Dar Al-Thaqafa for Publishing andDistribution,

[3] Hudood, A. Ahmad, E. 2025. An Analytical Study of the Effectiveness of Digital Forensic Investigations in Addressing Cybercrimes. Journal of Science and Technology. 30 (9). 68-76.

[4] Tabri, M. 2020. Expertise in Cybercrime. Journal of Al Hiwar Al Moutawassiti. 11 (3). 380-399.

★★★