Success and Failure in Cybercrime Investigations: Criminological and Procedural Determinants

Cybercrime is a widespread and persistent threat. Every day, crimes are committed online—ranging from hacking and malware attacks to fraud, hate speech, and other forms of abuse on social media. Most of these offences are never detected, and many are not even reported to law enforcement. Even when victims do come forward, investigations frequently fail due to the inability to identify the perpetrator. As a result, only a small fraction of cybercrimes lead to a successful prosecution, revealing a significant enforcement gap in the fight against cybercrime. Why do some investigations succeed, while others do not?

This research project seeks to answer that question. Drawing on real-life criminal case files from courts and prosecutors' offices in Poland, the project aims to identify the factors that increase or hinder investigative effectiveness. The research team will examine each case from two perspectives: the investigative actions taken by law enforcement and the behaviours or strategies used by offenders. The goal is to determine whether there are statistically significant differences in investigative tactics or offender behaviour between cases that led to prosecution and those that were discontinued due to failure to identify the perpetrator. The findings may inform future training, legislative reforms, and preventive measures.

The project uses a mixed-methods research design, combining quantitative and qualitative approaches. A representative sample of closed criminal cases from various court regions in Poland (both discontinued and adjudicated) will be analysed. From each case, anonymised data will be extracted concerning selected variables—identified through literature review and consultations with digital forensic experts and legal practitioners. These data will be subjected to statistical analysis, including logistic regression and decision tree models, to pinpoint which factors—such as types of evidence, procedural decisions, or offender conditions—are most strongly associated with investigative success or failure.

In parallel, a qualitative analysis will explore a subset of cases to develop crime scripts describing typical offender behaviour and investigative responses. This approach will also allow for a comparison between suspects' explanations and established criminological theories, helping to identify recurring patterns of motivation and decision-making.

Although the research is grounded in the Polish legal context, the challenges it addresses—such as data encryption, online anonymity, and cooperation with internet platforms—are universal. The findings will be relevant to researchers, legal professionals, and policymakers interested in improving the response to cybercrime.

This is a basic research project, not a technical or applied one. It does not aim to develop new tools or investigative procedures. Its aim is to generate deeper knowledge about how cybercrime investigations typically unfold, which factors influence their outcomes, and what can be learned from real investigative practice. Results will be shared in open-access publications, conference presentations, and publicly available reports. By focusing on actual case files—not just theory or statistics—this project aspires to offer practical, evidence-based insights that can help improve the effectiveness of cybercrime investigations in Poland and beyond.