SUMMARY OF THE DOCTORAL DISSERTATION

"Combating Cybercrime on the Example of Computer Fraud – Dogmatic and Evidentiary Problems in Pre-Trial Proceedings"

by Krystian Bartosz, M.A.

The subject of this doctoral dissertation is a comprehensive analysis of the phenomenon of cybercrime, with particular emphasis on the offence of computer fraud regulated under Article 287 of the Polish Criminal Code, as well as an assessment of the effectiveness of the existing legal framework and law enforcement practices in combating this type of crime. The aim of the dissertation is not only to characterize contemporary cyber threats but also to formulate de lege ferenda proposals intended to enhance the effectiveness of cybercrime prevention and prosecution.

The first part of the dissertation presents the theoretical foundations of the research problem, including the concepts of cyberspace and cybercrime, as well as an analysis of criminal offences against cybersecurity under Polish criminal law. Particular attention is devoted to the offence of computer fraud (Article 287 of the Criminal Code), as well as offences related to unauthorized access to information (Article 267), interference with data and information systems (Articles 268 and 268a), computer sabotage, and offences involving the creation and distribution of criminal tools and software (Articles 269 and 269b). This analysis made it possible to identify legal gaps and interpretative problems within the existing legal framework.

The dissertation further discusses the most common methods of committing cyber offences, including hacking, cracking, sniffing, phishing, skimming, ransomware attacks, and cryptojacking. Their mechanisms, prevalence, and significance for criminal investigations are examined, demonstrating the dynamic evolution of techniques employed by cybercriminals.

An important element of the study is a comparative analysis of legal regulations concerning cybercrime in selected jurisdictions, including the United States, the United Kingdom, the Czech Republic, Italy, France, Spain, Japan, and Germany. The comparative research enabled an assessment of the Polish legal framework against foreign solutions and facilitated the identification of potential directions for future legislative reforms.

The dissertation also evaluates the state of cybersecurity in Poland and the European Union on the basis of reports published by the Supreme Audit Office (NIK), CERT Polska, and the ENISA Threat Landscape. This analysis is supplemented by a discussion of specific cybersecurity incidents, including phishing campaigns, ransomware attacks, malware distribution, DDoS

attacks, and attacks targeting cryptocurrency wallets. These examples illustrate both the scale and the evolving nature of contemporary cyber threats.

A key part of the dissertation is devoted to proposals for legislative changes concerning the offence of computer fraud. The study proposes, inter alia, the criminalization of preparatory acts leading to computer fraud, the introduction of an aggravated form of the offence under Article 287 of the Criminal Code, and amendments concerning the penalization of identity theft. At the same time, the dissertation examines the possibility of extending the powers of law enforcement authorities in the field of non-procedural investigative activities while emphasizing the necessity of introducing safeguards against potential abuses.

The methodological section defines the research problem, hypotheses, and research methods applied in the study. The empirical research included interviews conducted with officers of the Central Cybercrime Bureau and forensic computer science experts. The findings were supplemented by an analysis of statistical data obtained from the Police and the Public Prosecutor's Office covering the years 2014–2024, which enabled an assessment of the dynamics of cybercrime, particularly computer fraud, at the national, European, and global levels.

The conducted research confirmed that the existing legal regulations do not fully address the challenges arising from the rapid development of cybercrime. Furthermore, the effectiveness of law enforcement activities remains limited due to difficulties in identifying perpetrators and the inadequacy of existing legal instruments in relation to contemporary technological realities. The conclusions of the dissertation indicate the necessity of legislative reforms and a broader application of modern technologies in the detection, investigation, and prosecution of cyber offences.

The dissertation constitutes an attempt to provide a comprehensive analysis of computer fraud in the context of contemporary cyber threats and serves as a basis for further research aimed at improving both the legal framework and its practical application in the field of cybercrime prevention and prosecution.