Abstract: This dissertation focuses on the systematization of techniques and processes related to the automation of threat modeling and vulnerability detection in modern, dynamic systems such as 5G networks. The evolution of 5G technology represents a significant shift from traditional, closed 3G and 4G telecommunications networks towards more open, Internet Protocol (IP)-focused structures. The dynamic nature of 5G architecture introduces new security threats, necessitating innovative threat modeling enhancements to the known techniques. Automating this process and modeling potential threats automatically remains a significant challenge for cybersecurity experts, service providers, and security offices. Solutions proposed in this works address the problem of automation of vulnerability prediction and threat modeling activities in complex systems like 5G networks. The study proves that it is possible to effectively model and prioritize threats in 5G networks considering their variable structure, and that adaptive computational algorithms can model and prioritize threats in real-time. Comparative analyses presented in the dissertation show that artificial intelligence can be useful for predicting vulnerabilities, generating threat related diagrams, and descriptions for threat models.

Keywords: Cybersecurity, Threat Modeling, 5G Networks, Vulnerability Detection, Automation, Artificial Intelligence, Network Security, Risk Mitigation