主动网络安全：愿景、模型和关键技术

张小松，朱宇坤，李雄，张永昭，牛伟纳，许峰华，何俊鹏，严然，黄世平
电子科技大学计算机科学与工程学院，中国成都市，611731

摘要：非合作性计算机系统与网络对抗构成了网络空间安全的核心挑战。传统网络安全技术主要依赖被动响应机制，在应对现实世界复杂多变的未知威胁时展现出显著局限性。本文提出“主动网络安全”理念，旨在通过融合技术手段与战略级防御体系，全面提升网络安全水平。该理念的核心假设是：网络对抗环境中的攻击者与防御者均为追求各自目标最大化的理性决策主体。本文引入博弈论分析攻防双方的复杂依存关系并优化其策略选择。基于该理念，构建了主动网络安全模型SAPC，旨在构建一种集威胁感知、分析、追踪和响应于一体的综合防御能力。该模型由4大核心组件构成：智感、透析、活现和反制。SAPC通过基于博弈论的对抗行为理论分析与策略优化方法，将对抗过程建模为博弈过程，建立兼具理论深度与实践指导价值的网络安全框架。SAPC标志着网络防御理念从被动防御到主动感知对抗的范式转变，有力推动网络安全技术向具有前瞻预测、预防控制和战略引导特征的新模式演进。

关键词：主动网络安全；智感；透析；活现；反制
https://doi.org/10.1631/FITEE.2500053