OntoCSD：基于本体的网络空间防御综合解决方案安全模型

武丹丹[1]，陈捷[2,3]，谢瑞云[3]，陈轲[1]

[1]电子科技大学成都学院计算机学院，中国成都市，610731

[2]西北工业大学网络空间安全学院，中国西安市，710000

[3]中国电子科技网络信息安全有限公司，中国成都市，610000

摘要：构建动态、灵活、智能的网络空间防御综合解决方案是一种新理念。为了解决传统静态防护方法在网络对抗环境下无法及时响应各种网络攻击或安全需求的问题，形成从“威胁发现”到“决策生成”的完整集成解决方案，我们提出一种基于本体的安全模型—OntoCSD，该模型使用Web本体语言来表示网络空间威胁监测、决策、响应、防御过程中所涉及的本体类和关系，并使用语义Web规则语言来设计防御推理规则。OntoCSD可以发现网络攻击、漏洞、安全状态和防御策略之间的潜在关系。进一步地，利用基于案例推理的人工智能专家系统快速生成详细、全面的决策方案。最后，通过肯德尔一致性系数和典型计算机网络防御系统中四个基于表征事实和本体推理的实验案例，验证了OntoCSD解决网络空间防御领域问题的一致性和可行性。OntoCSD支持自动关联和推理，能够为网络空间防御提供整体解决方案框架。

关键词：网络空间防御；集成解决方案；本体；基于案例推理（CBR）；计算机网络防御（CND）

https://doi.org/10.1631/FITEE.2300662