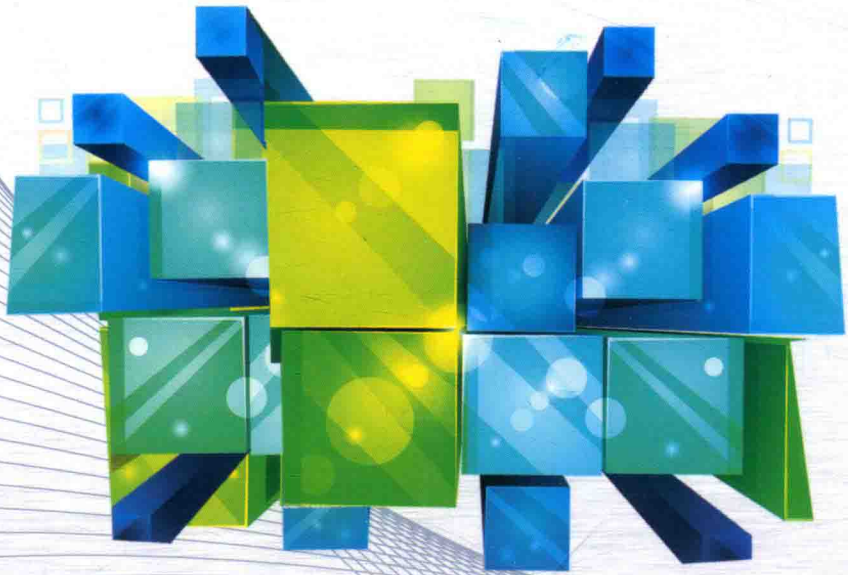
国家社会科学基金资助项目
网络与信息安全技术系列图书

网络生态系统动态演化

Dynamical Evolution of Cyber Ecosystem

王　刚　胡　鑫　伍维甲
吴　昊　陆世伟　著



西安电子科技大学出版社
http://www.xduph.com

国家社会科学基金资助项目
网络与信息安全技术系列图书

网络生态系统动态演化

Dynamical Evolution of Cyber Ecosystem

王 刚 胡 鑫 伍维甲 吴 昊 陆世伟 著

西安电子科技大学出版社

内 容 简 介

网络生态系统是在生物体免疫系统和社会公共健康领域的疾病控制的启发下，设想建立的一套类似于生物体免疫系统的网络安全防御体系。本书结合网络安全需求和生物体免疫机理，从复杂性科学和复杂系统理论的视角，研究了网络生态系统产生复杂性的机理及其动态演化规律。本书主要内容包括：绪论、网络生态系统的结构和演化规则、基于成熟度理论的系统动态演化、基于病毒传播与免疫理论的要素动态演化、基于集体防御的行动同步与控制、网络生态系统动态演化性能评估理论和方法。

本书基于作者所在研究团队多年来对网络安全领域的理论研究成果，适合于网络空间安全学科高年级本科和相关领域研究生理论教学，也可作为网络生态系统研究的参考书。

图书在版编目(CIP)数据

网络生态系统动态演化/王刚等著. —西安：西安电子科技大学出版社，2019.6
ISBN 978-7-5606-5307-5

Ⅰ. ① 网… Ⅱ. ① 王… Ⅲ. ① 计算机网络—网络安全 Ⅳ. ① TP393.08

中国版本图书馆 CIP 数据核字(2019)第 077016 号

策划编辑 李惠萍
责任编辑 苑 林 雷鸿俊
出版发行 西安电子科技大学出版社(西安市太白南路 2 号)
电 话 (029)88242885 88201467 邮 编 710071
网 址 www.xduph.com 电子邮箱 xdupfxb001@163.com
经 销 新华书店
印刷单位 咸阳华盛印务有限责任公司
版 次 2019 年 6 月第 1 版 2019 年 6 月第 1 次印刷
开 本 787 毫米×960 毫米 1/16 印张 13.5
字 数 218 千字
印 数 1～2000 册
定 价 34.00 元
ISBN 978-7-5606-5307-5/TP
XDUP 5609001-1

前　言

自20世纪90年代以来，网络经历了从最开始的Web 1.0时代，到21世纪初的Web 2.0时代，演化到如今朝着万物互联方向发展的Web 3.0时代，网络空间也从单纯影响人类生活方式转变为渗透作用于传统物理空间，社会治理、经济发展及关键基础设施的运行都离不开网络的赋能作用。网络空间的诞生使物理空间与虚拟空间的边界模糊不清，在刺激传统物理空间焕发新活力的同时，也将网络攻击的威胁从虚拟空间带向现实空间，使得网络空间的安全形势日益严峻。随着5G商用不断加速，美国对于争夺5G领先地位的焦虑感和紧迫感日益强烈。2019年4月，美国国防部国防创新委员会发布了《5G生态系统：对美国国防部的风险与机遇》报告，围绕“网络生态”主题，重点分析了5G发展历程、目前全球竞争态势以及5G技术对国防部的影响与挑战。

为应对当下十分猖獗的网络威胁势头，特别是近年来先进持续性威胁(Advanced Persistent Threat，APT)的发展，世界军事强国开始致力于研发“改变游戏规则”的技术，构建弹性的网络生态系统就是其中之一。美国是最早开启网络生态系统理论研究的国家，2011年3月他们就提出了利用自动化的集体防御建立弹性的网络生态系统，用以预测和防御网络恶意攻击，并能够在系统遭到破坏后快速恢复，从而保护地理上广域分布的国家基础网络。网络生态系统借鉴了生

物体免疫系统和社会公共健康领域的疾病控制机理，主要针对和解决网络安全的集体防御需求问题。近年来，移动目标防御、联动协同防御、蜜罐诱骗防御、入侵容忍防御、最优策略防御等网络安全非传统理念技术获得长足发展，使得构建弹性健康的网络生态系统成为可能。

关于网络生态系统，国内外学者认为，它是以生物体免疫系统和社会公共健康领域的疾病控制为启发，设想建立的一套类似于生物体免疫系统的网络安全防御体系。它利用网络设备内置的安全功能，通过自动化、标准化程序及协调一致的行动，使网络中的各要素形成一个集体行动、自动防护、自我愈合的健康、抗压和安全的生态系统。毋庸置疑，网络生态系统是典型的复杂系统，是一类有待深度挖掘的复杂系统，也是现阶段受到高度关注的前沿热点。网络生态系统具有复杂系统的适应性、不确定性和层次涌现性，生态系统的整体性、多样性、层次性、开放性和动态性，具有其特定的复杂机理和演化规则。动态演化是认知系统在运行过程中由平衡动态和演化动态的相互交替以及二者的统一所表现出来的活动。从复杂性科学和复杂系统理论的视角看，网络生态系统是一个蕴含复杂机理的动态演化系统，其动态演化过程是网络生态系统复杂机理的外在表现和维系复杂性的根本所在。

基于此，本书以复杂性科学和复杂系统理论方法为指导，结合网络安全集体防御需求开展网络生态系统理论研究，挖掘网络生态系统的复杂机理和动态演化规则。首先，从复杂性科学和复杂系统的视角系统阐述网络生态系统的概念内涵和基本属性，结合网络生态系统基础架构和能力分

析，定义了网络生态系统层级结构模型和层级作用关系，提出了网络生态系统演化规则。这些演化规则包括系统运行规则、要素联动规则和体系对抗规则，这些内容主要在第 1 章和第 2 章进行介绍。本书第 3～5 章分别从系统层面、要素层面和系统/要素协作关系等方面，提出了基于成熟度理论的系统动态演化、基于病毒传播与免疫理论的要素动态演化和基于集体防御的行动同步与控制。具体而言，基于成熟度理论的系统动态演化，通过建立演化模型定义了动态演化的关键过程域，从信息决策、要素协同和信息共享三个维度进行能力评估；基于病毒传播与免疫理论的要素动态演化，在分析要素演化过程和阶段的基础上，主要对节点增减、潜伏-隔离、复杂潜伏转移模式三种情况下的要素动态演化进行了研究；基于集体防御的行动同步与控制，通过建立行动同步与控制模型，区分同质与异质网络，分别研究了主动控制同步和自适应控制同步两种模式。本书第 6 章和第 7 章分别给出了网络生态系统动态演化性能评估理论和方法，建立了动态演化性能评估准则和指标体系，给出了设计的性能评估方法，阐述了方法如何实施以及运用等问题。

本书是全体参编作者和所在团队多年研究成果的总结和升华，由全体作者共同完成。在研究和撰写、完善的过程中，在读硕士研究生陈彤睿、陆世伟参与了部分章节内容的修改完善和全书的校稿工作，付出了大量辛苦且繁重的努力。同时，感谢西安电子科技大学出版社的李惠萍老师在本书的校稿和编辑方面投入的大量心血。网络生态系统理论是当前网络安全领域的前沿问题，相关研究尚处于起步阶段，可参考的资料有限，研究中的观点和方法多数属于探索性工

作；同时，由于各人对问题认知的角度可能存在一定的偏差，需要在后期工作中不断加强和完善的方面仍有很多。因此，虽然我们付出了很大的努力，但书中不可避免仍有疏漏与不妥之处，敬请读者批评指正。

本书作者邮箱：wglxl@nudt.edu.cn，欢迎交流。

作　者

2019年3月于西安

目 录

第1章 绪 论

1.1 网络安全背景

以“互联网”为代表的信息网络正以前所未有的速度重塑我们的生产、生活方式，与此同时，网络安全问题日益突出。从2010年“震网”(Stuxnet)事件到2013年“棱镜门”(Prism)事件，从2014年“能源之熊”事件到2017年“勒索病毒”(Ransomware)事件，再到2018年的“蜂巢网络”(Hivanet)，以先进持续性威胁(Advanced Persistent Threat，APT)为代表的一系列网络安全问题直接影响了网络的整体性能和稳定运行，并对公共社会秩序乃至国家安全造成威胁。目前，网络安全问题已经引起了各国的高度重视，各国普遍采取了应对措施。西方主要国家倡导以“网络生态”为主题的积极网络防御理念，试图构建一种具有弹性结构、可柔性重组，类似自然生态系统的信息网络体系——网络生态系统(Cyber Ecosystem)。2011年，美国在网络安全发展战略中率先提出“网络生态系统”的概念，即借鉴生物体免疫系统和社会公共健康领域的疾病控制机理，建立一套类似于生物体免疫系统的网络安全防御体系，利用网络要素内置的安全功能程序，通过自动化、标准化的一致行动，形成一个具有集体行动、自动防护、自我愈合等特征的，健康、抗压和安全的网络系统。2013年2月，欧盟发布《欧盟网络安全战略》，明确提出加强网络结构的弹性和网络防御能力。2014年1月，俄罗斯公布《俄罗斯联邦网络安全战略构想》(草案)，提出建立自主可控的网络安全机制。同年12月，英国发布《国家网络安全战略》，提出必须加强网络防御和网络反击能力。2015年4月，美国颁布《美国国防部网络安全战略(2015)》，指出以减少破坏性网络攻击来确保国家数据安全。同年12月，美国政府发布了《网络威慑战略》报告，从威慑视角再次强调加强网络安全防御能力和弹性健康的网络生态系统建设，提升遭受网络攻击后的快速恢复

能力。2017 年 1 月，美国发布《网络安全事件恢复指南》，旨在制订应对各类网络攻击活动的恢复方案和计划。同期，欧盟发布《欧盟安全事务进展报告》，将“网络犯罪”“网络攻击”等针对网络安全的行为列为威胁公共安全事务的主要挑战。2018 年 9 月，美国总统特朗普接连签发《国防部网络空间战略》概要和《国家网络安全战略》两份重要文件，前者重点是指导美军夺取并保持网络空间的优势，后者着重提出维护并保持网络空间安全的目标举措，二者均将网络威慑作为实现美国繁荣与安全战略目标的重要手段。

面对日益严峻的网络安全威胁，我国于 2014 年成立“中央网络安全和信息化领导小组”，明确提出信息化建设与网络安全要遵循“一体两翼，双轮驱动”的发展战略，加紧构建弹性和可持续发展的网络生态环境和网络生态系统。2015 年 6 月，国务院宣布成立网络空间安全一级学科，明确了网络安全的研究方向、内容和理论体系，网络生态化发展和安全度量是网络安全基础理论研究的重要内容。2016 年 11 月，国家出台《网络安全法》，明确从网络安全保护、网络信息服务和网络社会管理等方面，通过依法治网提升国家网络生态环境和性能。同年 12 月，国家发布《国家网络空间安全战略》，提出了我国网络空间安全及其发展的立场和主张，强调构建弹性的网络生态是重要的实现途径。2017 年 3 月，国家出台《网络空间国际合作战略》，提出在和平、主权、共治和普惠四项原则基础上，以构建网络空间命运共同体为目标，推动网络空间国际合作和共同抵御网络攻击。在军事领域，按照“一体双翼，双轮驱动”确保军队信息化建设先进性和安全性要求，国防和军队信息网络的安全性及信息网络对体系作战的支撑能力建设已成为重点，其重要途径就是构建健康和可持续发展的网络生态系统。2017 年 10 月，十九大报告提出，加快军事智能化发展，提高基于网络信息体系的联合作战能力、全域作战能力，有效塑造态势、管控危机、遏制战争、打赢战争，进一步给国防和军事领域网络生态建设提出了明确的方向和目标。2018 年，教育部更新我国高校学科目录，正式增设网络空间安全一级学科，从博士、硕士和学士各层次全方位加速培养新时代网络空间安全高层次人才。

网络生态系统汲取了新的网络防御理念，是基于自动化、互操作和身份认证的主动防御，通过网络诸要素整体协同行动来预测和防御包括不确定攻击在内的多类型网络攻击，将攻击后果最小化并恢复到可信状态。相比较而言，传统网络安全防御是以封控、堵漏、限制为重点和主要手段，基

本上是针对已知威胁的被动设防，安全防御(护)配置预先设定，安全策略独立实施。较之传统防御理念，网络生态系统的防御理念更强调集体防御、集体行动：通过网络中诸要素间的协同作用，实现整体态势感知、侦察、监视、攻击和防御，以减少网络遭受攻击的可能性甚至免受攻击，维持系统的健康稳定运行。随着世界范围内网络环境的复杂性和不确定性的日益增强，APT 攻击带来的全球网络安全及其防御问题日渐突显，如何实施对网络安全威胁及其防御行动过程的监视和有效控制？对于既定网络而言，通常可以通过断开关键节点间的链路来提升网络安全防御能力，但是这样会同步降低网络的业务承载能力。如何兼顾网络安全威胁防御需求和业务承载能力需求？如何根据复杂任务需求和现实网络安全，动态调控网络安全防御和业务承载状态？针对网络安全需求，开展网络生态理论和技术研究，科学设计网络生态机制和网络生态系统，是解决这些难题的重要途径。

网络生态系统是一个新兴事物，构建网络生态系统是一项复杂的系统工程，相关理论的研究应遵循复杂性科学和复杂系统理论方法。复杂性科学认为，“复杂性”是关于过程的科学而不是关于状态的科学，是关于演化的科学而不是关于存在的科学；而“复杂系统”是具有自适应能力的演化系统，其产生的复杂性机理及其演化规律需要采取复杂性科学方法，运用非还原论方法研究。网络生态系统理论研究，以网络安全需求为牵引，从网络生态系统产生的复杂性机理及其演化规律入手，聚焦系统的演化过程和动态特性。通过网络生态系统理论研究，首先可以理清基于集体行动的网络生态系统集体防御机理，为解决现实网络安全问题，开展网络空间治理提供理论方法支撑；其次，建立层次清晰、功能明确的网络生态系统结构模型和动态演化规则，为网络安全集体防御行动组织指挥和建立健康有序的网络生态系统提供体系设计参考依据；此外，通过建立和解析网络生态系统的系统运行规则，提升网络生态系统应对不确定或蓄意网络攻击的能力，实现对现实应用网络的有效控制，均衡网络在遭受攻击情况下的业务承载能力；最后，推进网络生态系统理论深化发展，形成网络生态系统动态演化性能评估理论和方法体系，加速网络生态理论向实践应用的发展。

1.2 网络安全集体防御

网络安全防御通过采取漏洞检测、身份认证和运行监控等措施抵御敌

方恶意网络攻击，保障我方网络安全，是网络行动的基础和前提。网络安全防御手段主要包括网络设备安全监管、网络病毒防护、网络攻击检测、终端漏洞检测、系统补丁更新、重要数据防护、网络防护、信道防护、流量控制和网络访问审计等。例如，通过部署病毒防护系统，针对网络病毒的传播感染规律和发展趋势，制定针对性的病毒杀除和防护策略，属于网络安全防御的病毒防护手段；在局域网各端口处部署防火墙，严格审计、控制出入各域网络的数据包，加强安全防护管理，属于网络安全防御的网络防护手段；部署补丁分发服务器和为相应操作系统和软件漏洞进行补丁操作，降低网络恶意威胁风险，提升网络安全防御能力，属于网络安全防御的系统补丁更新防护手段。网络安全防御主要包括可信计算防御、自主可控防御、动态目标防御和集体防御等安全防御策略。具体而言，这四种防御模式各有如下特点：

(1) 可信计算防御，这是集运算与防御并存的防御新模式，通过采用密码实施身份识别和保密存储，实时识别“敌我”身份，实现在网络运算可控可测的同时，实施网络空间安全防御。

(2) 自主可控防御，指依靠自身研发设计，全面掌握核心技术，实现网络从硬件到软件的自主研发、生产、升级、维护的自主可控、安全可控，防止恶意后门并不断改进和修补漏洞。

(3) 动态目标防御，即改变传统网络相对静态的运行环境，通过动态改变网络设置和配置，使得设备或网络在一定程度上以时间的函数进行变化，动态抵御网络攻击。

(4) 集体防御，这是基于自动化、互操作和身份认证的主动防御，通过网络诸要素的整体协同来预测和防御包括不确定攻击在内的多类型网络攻击，并将攻击后果最小化。

2011 年 3 月，美国国土安全局首次提出利用自动化的集体行动建立弹性的网络生态系统，强调运用“自动化、互操作和身份认证”手段提升网络运行速度、优化决策、态势感知和隐私防护等能力，预测和防御网络恶意攻击，并能够快速恢复，实现网络安全的分布式安全防御。2014 年 3 月，美国空军公开征集“网络防御系统、网络防御分析系统、网络安全漏洞评估系统、网络指挥控制任务系统、内部网络控制系统和网络安全与控制系统”等六类网络空间安全防御设计方案，旨在提高美国空军应对网络攻击的快速响应和恢复能力。2017 年 4 月，美军在原有分布式安全防御基础上，提出基于集体行动的新型分布式网络安全体系，与传统网络安全系统相比，基

于集体行动的新型分布式网络安全体系实现了网络安全防御能力的“优化倍增”，尤其针对大规模集群攻击的安全防御效果更佳。在该体系中，网络中任意节点一旦探测到网络攻击行为，将实时告知全网其他网络节点，迅速封锁网络病毒的攻击源头及其传播路径，并将网络攻击(病毒)阻断、隔离在受损的特定网络区域内，实现全网免疫；同时，通过启用相邻网络节点的备份信息，快速恢复网络运行，提升网络运行效率和安全性能。网络安全防御突破常规思维和传统防御理念，区别于传统的筑高墙、堵漏洞和防外攻的安全防御模式，网络安全防御应逐步形成基于网络安全防御集侦察预警、指挥决策、防御应急、反击进攻和保障力量于一体的综合防御。

从现阶段分析，集体防御是网络安全和网络行动的重要保障，网络安全由网络诸要素通过相互协同、共同作用抵御随机或蓄意安全威胁/攻击，并对安全威胁/攻击行动做出响应和恢复。网络行动包含通过运用网络诸要素达到预期目的而采取的网络空间安全态势感知、侦察、攻击和防御等各类活动。网络安全集体防御依赖于构建弹性的新型网络系统，从要素关联和作用关系来看，这种新型网络系统能通过诸要素间的相互关联、协作共享，共同构成一个连续、线性的动态网络，通过集体防御提升网络的安全可靠、自愈修复和态势感知等能力，实施网络的实时动态安全防御。

网络安全集体防御主要包括集体防御主体、集体防御策略和集体防御流程三大要素。

(1) 集体防御主体。集体防御主体包括制定、监控和实施网络安全集体防御行动的决策者、管理者和执行网络安全集体防御的网络设备、用户等集体防御的物理实体，以及网络安全集体防御任务和行动等集体防御的虚拟实体。各物理实体和虚拟实体之间围绕集体防御目标相互关联、集体协同。

(2) 集体防御策略。网络参与方(特别是网络设备)要求具备自动化、互操作和身份认证等三种相互依存的关键能力，网络的状态、特征和安全防御需求制定等内容可以转化为相应的策略描述语言。主要防御策略包括稳健防御策略、主动防御策略和弹性防御策略三类。具体而言，稳健防御策略即网络诸要素基于自身的安全性能，实时接收来自管理中心的任务和指令，为网络提供基本的、稳固的安全防御能力；主动防御策略即通过主动分析、观察和总结，预判敌方网络攻击/威胁规律，制定相应的安全防御策略，抵御不确定、潜在的网络攻击/威胁；弹性防御策略即在监控、追踪网络攻击/

威胁目标过程中，通过提供连续不断的安全防御，最大限度地保障自身重要节点的安全，实现快速修复。

(3) 集体防御流程。集体防御流程通常可以划分为监视阶段、检测阶段、防御阶段和修复阶段四个阶段，如图 1.1 所示。在集体防御流程中，各阶段的同步有其具体目标和特点。在监视阶段，诸要素协调有序、信息共享，对网络进行安全动态监视，实现网络安全实时动态监控；在检测阶段，诸要素交互共享网络攻击源信息，对网络进行安全分析检测，实现网络空间安全威胁的精确侦察检测；在防御阶段，诸要素优势互补、态势共享，对网络进行安全防御，实现网络安全的态势感知、动态防御；在修复阶段，诸要素相互协调、共同作用，对受攻击后的网络进行安全修复，实现网络安全的实时动态自愈修复。

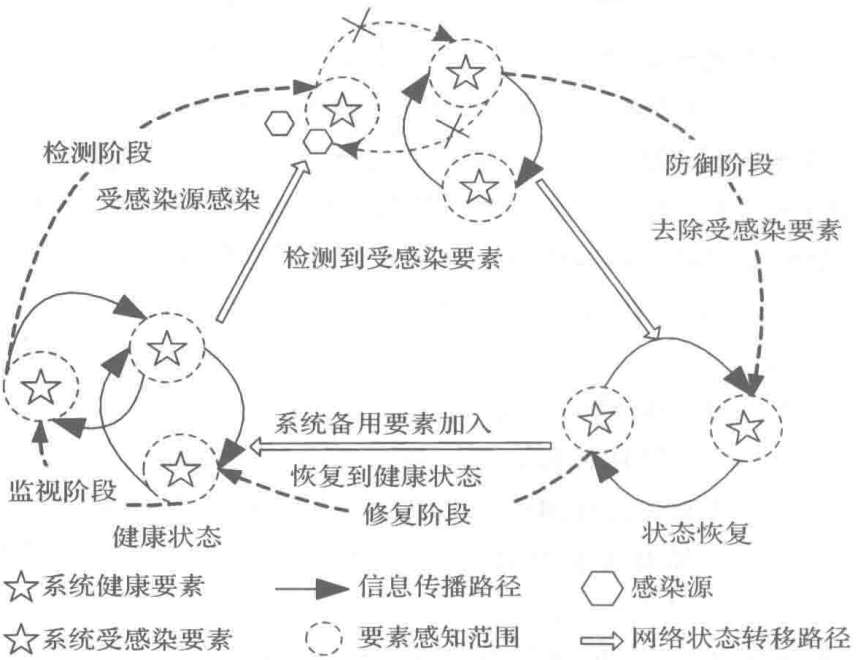


图 1.1　网络安全集体防御流程

1.3　网络生态系统基本概念

1.3.1　网络生态系统基本内涵

网络空间是融合物理域、信息域、认知域和社会域的人造虚拟空间，通