# 基于超网络的网络安全事件连锁演化模型

姬逸潇[1,2], 吴晨思[2], 杨 粟[2], 郭 敏[3], 张玉清[1,2]

[1]西安电子科技大学 网络与信息安全学院 西安 中国 710071
[2]中国科学院大学 国家计算机网络入侵防范中心 北京 中国 101408
[3]北京计算机技术及应用研究所 北京 中国 100000

**摘要** 由于网络的强大的互通性, 安全事件的发生常常伴随着其他安全事件的触发, 形成连锁反应, 造成一定的危害和经济损失。本文从系统论的角度出发, 研究网络安全事件之间的不同关联, 分析安全事件演化的不同模式, 以点、链、网的概念为基础, 引入超网络进一步建立四层演化模式的概念, 并针对安全事件的不同演化模式进行了详细分析; 最后通过实际案例说明了安全事件演化模型的可行性。研究结论对于预防安全事件影响的扩大, 以及危害的宏观预警具有一定的积极意义。

**关键词** 网络安全事件; 超网络; 连锁演化
**中图法分类号** TP309 DOI 号 10.19363/J.cnki.cn10-1380/tn.2019.01.08

# Network Security Event Chain Evolution Model Based on Super Network

JI Yixiao[1,2], WU Chensi[2], YANG Su[2], GUO Min[3], ZHANG Yuqing[1,2]

[1] School of Network and Information Security, Xidian University, Xi'an 710071, China
[2] National Computer Network Intrusion Prevention, University of Chinese Academy of Science, Beijing 101408, China
[3] Beijing computer technology and application institute, Beijing 100000, China

**Abstract** Due to the strong interoperability of the network, the occurrence of security incidents is often triggered by other security incidents, forming a chain reaction, causing certain harm and economic losses. From the pers pective of system theory, this paper studies the different relationships between network security events, analyzes the different modes of security event evolution, and introduces the concept of point, chain and network to introduce the concept of four-layer evolution mode. The different evolution modes of security events are analyzed in detail. Finally, the feasibility of the security event evolution model is illustrated by actual cases. The conclusions of the study have certain positive significance for preventing the expansion of the impact of security incidents and the macro-warning of hazards.

**Key words** network security event; super network; chain evolution

## 1 引言

近年来, 随着计算机技术和通信技术的迅速发展以及用户需求的不断增加, 计算机网络规模日益庞大, 应用系统日益复杂。网络安全威胁的范围和内容不断扩大和演化, 网络安全形势与挑战日益严峻复杂[1]。

网络安全事件作为网络安全领域的重要研究内容, 发生频率呈现逐年增长的趋势, 对各个领域的影响也在不断增强[2]。网络安全事件是指由于自然或者人为以及软硬件本身缺陷或故障的原因, 对信息系统造成危害, 或对社会造成负面影响的事件。近年来对社会影响较为深远的安全事件, 比如 2016 年 10 月, 美国遭遇史上最大规模的 DDoS 攻击, 恶意软件 Mirai 控制的僵尸网络对美国域名服务器管理服务供应商 Dyn 发起 DDoS 攻击, 从而导致许多网站在美国东海岸地区宕机, 如 GitHub、Twitter、PayPal 等, 用户无法通过域名访问这些站点; 2017 年 5 月 WannaCry 勒索病毒的全球爆发, 以类似于蠕虫病毒的方式传播, 至少 150 个国家、30 万名用户中招, 造

**通讯作者:** 张玉清, 博士, 教授, zhangyq@nipc.org.cn。
本课题得到国家重点研发计划项目(No. 2016YFB0800700)、国家自然科学基金项目(No. 61572460, No. 61272481)、信息安全国家重点实验室的开放课题(No. 2017-ZD-01)、国家发改委信息安全专项项目[No. (2012)1424]和国家 111 项目(No. B16037)的资助。
收稿日期: 2018-09-30; 修改日期: 2018-12-03; 定稿日期: 2018-12-07

成损失达 80 亿美元, 已经影响到金融, 能源, 医疗等众多行业, 造成严重的危机管理问题; 2018 年 3 月, Cambridge Analytica 公司被爆出对 Facebook 用户的信息进行窃取[3], 造成近 5000 用户隐私信息泄露, 甚至对美国大选的公正性产生了影响。

网络安全事件既存在内在联系, 同时又相互影响[4], 导致不同事件的发生并形成连锁反应, 使得安全事件的性质更为复杂, 在更长的持续时间内, 造成的危害更加严重。安全事件的演化规律, 不仅包括单个安全事件的演化规律, 还包括安全事件之间产生连锁反应的演化规律, 认识这些演化规律对于网络安全态势[5]的预测和感知具有非常重要的意义。

目前对网络安全事件的研究主要针对在不同的攻击类型和受到的危害, 少有交叉。网络安全事件根据其发生过程、性质和机理, 可基本分为有害程序事件(MI)和网络攻击事件(NAI)两种类型, 有害程序事件(MI)和网络攻击事件(NAI)具体向下分类[6]如表 1 所示。

**表 1 网络安全事件具体分类**

**Table 1 Specific classification of network security incidents**

| 有害程序事件(MI) | 网络攻击事件(NAI) |
|---|---|
| 计算机病毒事件(CVI) | 拒绝服务攻击事件(DOSAI) |
| 蠕虫事件(WI) | 后门攻击事件(BDAI) |
| 特洛伊木马事件(THI) | 漏洞攻击事件(VAI) |
| 僵尸网络事件(BI) | 网络扫描窃听事件(NSEI) |
| 混合攻击程序事件(BAI) | 网络钓鱼事件(PI) |
| 网页内嵌恶意代码事件(WBPI) | 干扰事件(II) |
| 其他有害程序事件(OMI) | 其他网络攻击事件(ONAI) |

安全事件的研究作为网络安全评估的重要组成部分, 将系统论的概念引入安全事件也具有十分积极的意义。系统论[7]是研究系统的结构、特点、行为、动态、原则、规律以及系统间的联系, 并对其功能进行数学描述的。系统论的主要思想就是以系统为对象, 从整体出发来研究系统整体和组成系统整体各要素的相互关系, 从本质上说明其结构、功能、行为和动态, 以把握系统整体。

本文主要贡献为从系统论的角度出发, 建立不同种类安全事件之间的关联, 研究安全事件的演化过程, 提出了安全事件连锁演化四层框架体系, 帮助决策者关注不同模式的危害, 进一步加强网络安全。

本文从点、链、网、超网络的四个概念角度对安全事件进行描述, 通过实际安全事件案例, 对所提出的连锁演化框架体系进行验证, 证明了所提出的框架的可行性。最后对研究内容进行总结, 说明安全事件连锁演化框架体系的应用价值, 并展望本研究的后续工作。

## 2 研究现状

### 2.1 网络安全事件的研究现状

历史上对于网络安全事件的研究在不同的领域都有所建树, 但是整体来看都较为分散。

Saeed Salah 等人[8]在对安全事件的分析工具进行了阶段性总结, 代表性的包括 Swatch、SEC、OSSEC 等工具; 李明桂等人[9]提出了一种基于大数据的安全事件挖掘框架, 从海量、多源、异构的原始数据中, 提取有效的安全事件, 发现安全风险、潜在威胁和未知攻击; Robert F. Erbacher 等人[10]提出了一种基于图的跟踪挖掘方法, 用于理解所收集的事件检测和响应数据, 从操作轨迹构建数据分类的有用模式。可以基于规则来构造有限状态机以自动化数据分类。根据跟踪构建状态机, 然后评估开发状态机的有效性和状态机的性能; 蔡晓志等人[11]通过以安全事件识别为始发点, 以安全事件生命周期为思路, 以安全管理和安全技术为支撑, 构建安全事件生命周期管控体系。

安全事件应急响应是安全事件研究的一个重要领域, 早在 2004 年, 冯涛等人[12]提出了一套网络安全事件应急响应联动系统的基本模型, 可以充分协调地理分布的资源协同应对网络安全事件; 在 2011 年, 王瑞刚等人[13]通过对网络安全事件特点的分析, 指出了网络信息安全事件应急响应(NISIER)体系的关键所在, 提出了一种 NISIER 体系结构——“8641”层次结构, 并进一步阐明了该体系的联动运行方式; 2018 年, 赵旭等人[14]为了解决网络安全应急响应系统和网络安全应急管理平台问题, 提出基于 Web 的网络安全应急管理平台的安全架构方法, 该方法通过使用参数化语句的存储过程, 过滤危险信息。

通过对以上安全事件研究现状的分析, 对网络安全事件的研究主要集中在对响应模型的提出, 并没有对安全事件之间的内在关联的机制和原理进行进一步揭示, 即安全事件时空语义的关联关系; 同时主要的数据来源集中在入侵检测数据和日志数据等方面, 并没有针对于网络安全事件的文字数据的分析和研究。

### 2.2 连锁演化机理研究现状

连锁演化过程, 指某种事物或事件的发展和变化依赖于其他某种或某些事件或事物, 不同的事件或事物之间存在因果关系。

在之前的关于连锁演化机理的研究中, 罗毅等人[15]针对电网的连锁故障, 提出了一种基于图论的模式搜索方法, 根据实时的网络拓扑结构和潮流运行方式, 建立系统潮流状态图; 刘友波等人[16]为揭示连锁故障过程中呈现的微观脆弱环节, 提出多层时序运行演化模型对连锁故障进行模拟, 可以较为真实地反映电网运行、发展、与连锁故障的关系; 荣莉莉等人[17]基于灾害系统论, 在单一突发事件发生机理的基础上, 研究了突发事件连锁反应与孕灾环境的关系, 归纳出了四类突发事件的孕灾环境, 提出了突发事件之间的连锁反应机理并构建了突发事件连锁反应模型;

王宁等人[18]结合知识元在描述突发事件领域事物知识方面的优势, 将共性知识元模型引入到事件演化路径推理中, 建立元事件模型和客体模型, 利用不同属性间关系获取事件和客体的破坏函数、作用函数、触发函数和影响函数, 从而提出一种通过属性和映射关系预测连锁反应演化路径的方法; 朱政威等人[19]则提出以复杂系统理论和复杂网络理论为基础并借鉴灾害链的相关研究, 分别针对单一突发公共安全事件、突发公共安全事件链式扩散和突发公共安全事件网络扩散的特征、共性进行探索, 建立事件发生、演化和扩散的复杂系统动力学模型; 张荣等人提[20]出一种基于 Hopfield 神经网络的突发事件连锁反应路径推演模型。该模型用 Hopfield 神经网络表示一般的突发事件网络, 用 Hopfield 神经网络的运行规则表示突发事件连锁反应的原理, 并设置神经元阈值, 将突发事件连锁反应路径的推演过程映射为 Hopfield 神经网络的演化过程。

通过对以上连锁演化研究现状的分析, 可以看出, 对于连锁演化机理的应用和研究大部分集中在电力、自然灾害、突发事件等领域, 在网络安全事件的研究中还没有进行过实际应用。而不同的网络安全事件之间也存在着不同层次的内在联系, 对网络安全事件之间的连锁演化机理的研究对于网络安全态势的觉察、理解和投射都具有非常积极的意义, 对网络安全事件引入连锁演化的概念, 是具有的创新性的选择。

## 3 安全事件连锁演化框架体系

安全事件对社会各领域都会产生巨大的影响, 很多人对安全事件产生的危害进行了研究, 对直接危害的研究包括数据泄露、系统瘫痪、硬件破坏等, 对间接危害的研究包括经济损失、社会恐慌心理、政治因素等[21-26]。随着社会的发展, 各环节之间的关系日趋紧密, 安全事件的性质发生了根本性的变化, 传统以上的静止的, 孤立的事件已经越来越少, 安全事件不仅自身演化, 还有不同事件之间的蔓延、耦合、转化和触发, 以及形成的衍生和二次危害, 构成了一个复杂的系统。

通过对上述的研究成果及不同安全事件典型事例的研究, 从系统的角度出发, 本文建立了包含点、链、网、超网络的安全事件演化模式框架[27]。如图 1 所示。

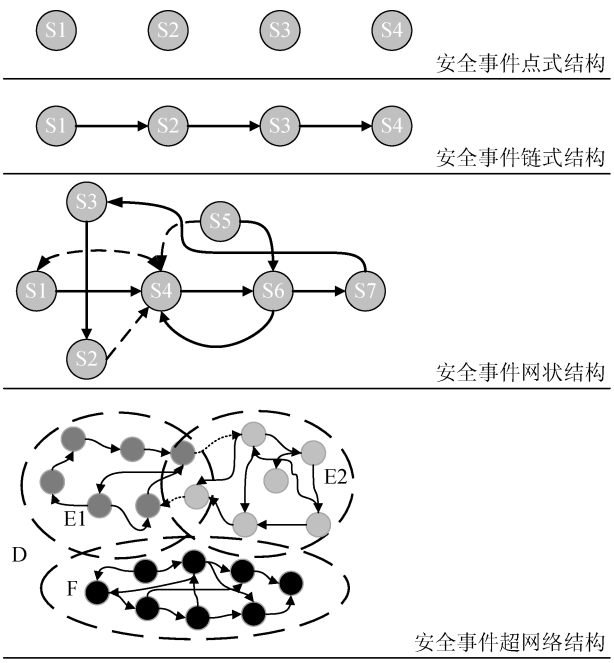



**图 1 安全事件 4 层演化模式**

**Figure 1 Four-hierarchies evolution model of Security incident**

该框架由四个层次构成, 安全事件点、安全事件链、安全事件网和安全事件超网。图 1 中的 Si 表示某一具体安全事件, 实线表示安全事件之间实际发生的演化过程, 虚线表示不同安全事件之间有发生连锁反应的趋势, 安全事件超网络结构中的 E1 区域和 E2 区域代表两种不同的网络空间环境, 而 F 区域则代表基础设施环境。第一层表示的是单个事件的演化模式, 第二到四层则表示安全事件之间的连锁反应模式, 其中, 安全事件链是一种线状辐射结构; 安全事件网则比链式结构更为复杂, 呈网状辐射, 表示的危害区域较大; 而安全事件超网络, 表示的危害区域更大, 是安全事件网络的网路。

### 3.1 安全事件的点式演化模式

点演化模式是最为基础的演化模式, 即安全事件发生后, 以点的方式传播, 是指其只有自身的演化, 不引起其他事件的发生, 有一部分的安全事件

都属于该层次的演化。

中央网络安全和信息化委员办公室的消息网络安全事件主要分为四个等级特别重大网络安全事件、重大网络安全事件、较大网络安全事件、一般网络安全事。以上对应的突发事件, 以这些突发事件为代表的各类突发事件都属于该层次[28]。

针对此类型的网络安全事件的演化研究, 大多探讨网络安全事件发生原因, 如苏剑飞、王景伟[29]从有机可乘的系统漏洞、形同虚设的口令和无线互联功能的计算机及其外围设备窃密等方面考虑攻击技术的发展原因, 并以此作为安全事件的演化基础; 应向荣[30]进一步说明了主动防御工具研发的关键环节, 强调了主动防御工具的重要性以及工具研发的新趋势, 认为安全事件的发生原因跟主动防御工具的研发有很强的关联性。

对于单个安全事件, 由于其突发性、不可预见性的特点, 发生时不可避免的, 因此就一定要加强安全事件应急机制[31]、应急响应等工作建设, 包括事件发生前的应急预案、法律法规的健全和完善, 事中的快速有效的应急响应机制、事后的总结和完善机制等。

### 3.2 安全事件的链式演化模式

安全事件发生后, 如果以链的方式传播, 则指的是两个安全事件之间在一定的触发条件下建立了一定的关系。2012 年, 荣莉莉等提出了突发事件链的理论概念: 突发事件链就是一系列突发事件相继发生的现象。随后张荣[32]有把突发事件链定义为: 一种突发事件启动另一种突发事件的现象, 更突出强调了事件发生之间的关联性。该定义的出发点是针对突发事件的, 网络安全事件由于其发生原因、性质以及演化规律, 在本质上也属于突发事件的范畴。

所以将突发事件引申并且具象到网络安全事件, 则安全事件链是指一个安全事件启动(触发)另一个安全事件的现象, 安全事件相继触发而形成的链式结构。链式结构是指某些存在触发条件的安全事件之间, 由一时间触发与其相关的事件, 依次相继发生其他安全事件而形成的单一安全事件链。这类演化模式的最大特点是相继发生, 前一事件为后一事件发生的原因。

随着社会发展, 不同网络安全领域的事件之间的耦合、转化和触发, 将使网络安全的态势变得更为严峻, 同时加速了危害的扩散。

安全事件链的形成, 是一个安全事件的发生, 导致后一个事件的触发。这与事件发生所处的网络空间环境尤其是网络资源环境密切相关。单一事件的发生时无可避免的, 但如果意识到可能产生连锁反应的后果, 就能够在前一事件发生后, 积极采取相应的措施, 切断其能引发后一连锁事件链。因此, 需要及时发现和识别可能存在的链式反应环境, 进行危害预警, 进一步提高降低连续危害的可能性。

### 3.3 安全事件的网状演化模式

网络空间环境指的是网络空间的软硬件设施以及在网络空间中流转的数据内容。在结构不同的网络空间环境中, 多个事件能够引发一个安全事件的发生, 此事件也可能引发多个其他安全事件的发生, 即多条安全事件链条交叉到一起, 从而形成网状辐射。安全事件网状演化是指安全事件通过具体网络空间环境相连而形成的网络, 网络节点是安全事件, 事件之间是否存在触发关系决定了对应网络节点是否有连边的可能。

最常见的网络空间环境本身就是网络。同一或同类安全事件在相互关联的基础设施或数据内容中以网络的形式进行蔓延、传播和转化, 网络的结构为现实网络设施的拓扑结构, 如以太网、物联网络、移动网络[33]等, 大面积的移动设备断网事件、物联网设备[34]的崩溃事件、计算机病毒的传播事件等。从本质上说, 这种类型与第一层的安全事件点是相似的, 都是一个事件本身的扩散, 只不过其物理载体本身构成了网络, 而使得危害得以进一步加深。目前, 研究较多的是以基础设施网络为基础的演化和传播, 如利用网络理论对电力供应、病毒传播、流言传播等进行建模。

另一种是网络空间环境本身不是网络, 但构成了不同安全事件相互触发的条件, 形成了安全事件的网络。该网络与网络资源环境是紧密相关的, 例如蠕虫病毒不同的传播环境, 像邮件系统、文件共享系统、软件供应链等均属于此种情况。

安全事件网比链更复杂。首先, 链呈线状辐射, 网是网状辐射, 结构形态更复杂; 链关注的是安全事件之间的一种可能连锁路径, 而网关注的是区域网络空间环境内所有安全事件之间的触发关系, 更全面; 网是由链组成。其次, 安全事件网的网络空间环境也更为复杂, 如果说链式演化的网络空间环境是一维的, 则网状演化的整体环境是多维的。从宏观的角度来看, 由于不同区域对应不同的网络空间环境, 因此, 同一事件发生在不同的区域网络空间环境中可能产生不同的安全事件网络。

### 3.4 安全事件的超网络演化模式

超网络(super network)概念是在超图理论[35]的基础上提出和进一步发展的, 目前超网络的定义是指

网络套着网络的多层、多级、具有多属性和多目标的网络。超网络具有增长和择优连接等优势, 可以动态地描述复杂系统[36], 最重要的是超网络存在演化特性。

安全事件一方面依托一定的基础设施完成自身演化和发展, 另一方面, 安全事件通过区域网络空间环境[37]与其他安全事件建立触发关系, 形成安全事件网。

因此, 利用超网络概念去建立描述安全事件连锁演化模型是非常合适的。

### 3.4.1 超网络概念

在异构的实际环境中, 用一般的网络图结构并不能完善地描述真实世界中网络特征。

针对超大规模的网络系统的研究中[38], 会出现物流网络与信息网络、资金网络相影响的问题, 或者深层网络中的更为具象的问题。如果利用偏向于工程的方法来分别解决各个网络之间的问题, 甄别各个网络之间的关系就变得更困难, 如何处理超越一般网络的网络系统的问题成为各个领域的研究热点。

以超图理论为基础, 最早提出“超网络”概念的Sheffi[39], 美国科学家Nagurney[40]等在处理上述交织的网络时, 把高于而又超于现存网络的网络, 称为超网络, 使得它的含义开始明朗。

超网络可以表示[41]为图 $G=(N,L)$, 其中, $N=\{n_1,n_2,\cdots,n_k\}$ 是其节点集, $n_i$ 表示 $G$ 的一个节点, $k$ 是超网络中的节点实体个数, 下标 $i=1,\cdots,k$ 是节点的唯一识别; $L=[l_{ij}]$是超网络中表示节点之间交互关系的链路矩阵, 链路 $l_{ij}$ 表示 2 个节点 $n_i$ 和 $n_j$ 之间的超边, 即两节点之间的交互关系 $(n_i, n_j \in N, i \neq j)$。

以上是对超网络的数学描述, 当超网络的节点和超边等元素被赋予实际意义后, 会具备下列一种或几种特征[42]:

(1) 多层次性: 例如安全事件可以从安全事件层和基础设施层两个角度进行描述。

(2) 多级特征: 例如在安全事件中, 有影响力不同级别的事件, 同级(水平)和级间(垂直)都存在联系。

(3) 流量的多维性: 例如安全事件的内在关系中, 既有简单的直接因果关系, 也存在间接因果关系。

(4) 多属性: 例如安全事件本身有很多附属的属性, 经济影响、舆论影响、触发原因等不同属性。

(5) 拥塞性: 例如在超网络中, 某个安全事件的节点或超边出现了中断, 都会出现网络拥塞的情况。

(6) 协调性: 例如从安全事件的角度来讲, 全局事件和单位事件在超网络中扮演的因果角色需要不断地调整和改变。

### 3.4.2 安全事件连锁演化模型的建立

随着现代社会的发展, 同类基础设施的联系十分紧密, 形成了特定的网络结构, 如物联网、自组织网络、LTE 网络等, 这些网络结构不仅为同类安全事件的触发建立了条件, 而且使得不同类型的安全事件之间的触发关系也变得十分复杂。

安全事件网络是安全事件超网络的一种表现形式。在表面上, 安全事件超网络也是一种安全事件网络; 然而, 它与安全事件网络的根本区别在于, 除了时间以不同的网络形式存在外, 其网络空间环境也以不同的网络形式存在, 并且事件网络与网络空间环境的网络之间相互影响, 形成安全事件超网络结构。如图 2 所示。

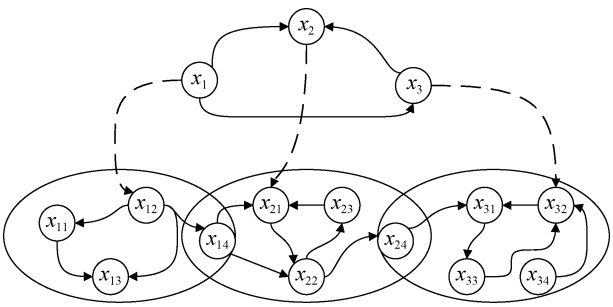



**图 2 安全事件超网络模型**

**Figure 2 Super network evolution model of Security incident**

安全事件超网络有着明显的层次特点, 由事件层和基础设施层构成, 分别对应图 3 的上层和下层, 事件层中的 $x_1$, $x_2$, $x_3$ 表示事件集 $m=\{x_i \mid x_1,x_2,x_3,\cdots,i=1,2,3,4,\cdots\}$ 中不同的安全事件, 基础设施层中的 $x_{1j}$, $x_{2j}$, $x_{3j}$ 表示对应的基础设施网络或网络空间环境中的节点集 $n=\{x_{ij} \mid x_{11},x_{12},x_{13},\cdots,x_{21},x_{22},x_{23},\cdots,x_{31},x_{32},x_{33},\cdots, i=1,2,3,4,\cdots,j=1,2,3,4,\cdots\}$ 中的具体环境节点。事件层表示安全事件之间的触发关系, 基础设施层则是实际设施的拓扑结构或者抽象概念结构。安全事件超网络描述了在一定基础设施结构的条件下, 各类安全事件发生连锁反应的可能性。安全事件的传播除了通过触发其他安全事件来体现外, 还有其自身在一定空间条件下的传播, 而这两种传播又是相互交织, 相互影响的, 把两者统一到一个框架下, 不仅能更清晰地了解安全事件自身连锁演化的规律, 同时也能分析特定环境下不同安全事件相互触发关系, 达到识别风险和危害预警的效果。

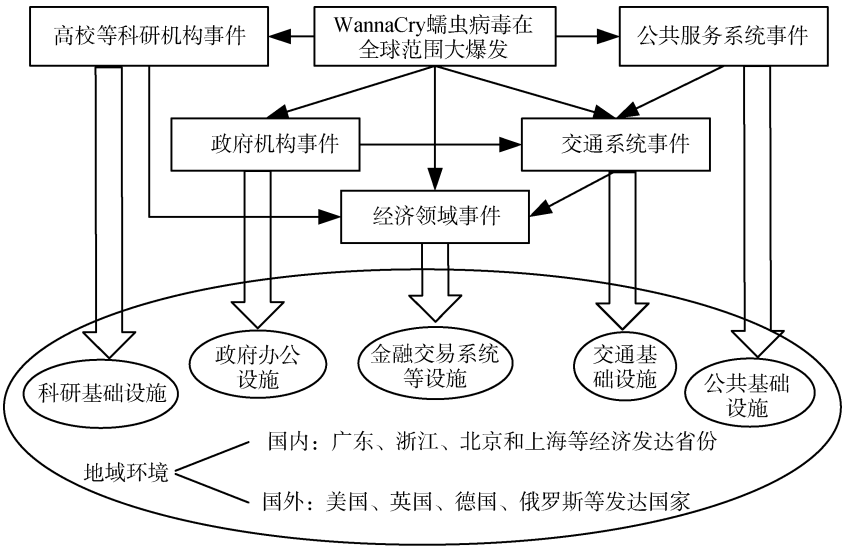



**图 3　基于影响扩散的安全事件超网络模型**

**Figure 3　Super-network evolution model of Security events based on impact diffusion**

## 4　基于安全事件的超网络演化模型构建方法

### 4.1　定义单位安全事件

单位安全事件(也称为原子安全事件或简单安全事件)是指在网络空间环境中, 以微观角度直接观察到的、最基本的不能再分解的安全事件, 任何安全事件从宏观角度都可以表示为若干个单位安全事件的并集集合。一个单位安全事件可以是某一个单位安全事件的原因, 也可以是某一个安全事件的结果[43]。

如针对 2017 年 5 月 WannaCry 勒索病毒的全球爆发这一广受关注的安全事件, 从微观角度上看, 将其中“WannaCry 勒索病毒的全球爆发”定义为单位安全事件 A, 而事件 A 的后续影响事件, 即“国内高校众多实验数据和毕业设计被锁定”被定义为单位安全事件 B, “Petya 蠕虫病毒爆发”定义为单位安全事件 C, 事件 A 的触发原因事件, 如“永恒之蓝漏洞武器的公开”定义为单位安全事件 D。

可见事件 B 与事件 C 可以看做事件 A 的结果, 同时事件 A 可以看做事件 B 与事件 C 的发生原因; 事件 A 可以看做事件 D 的结果, 同时事件 D 可以看作事件 A 的发生原因。

从宏观的角度上看, “WannaCry 勒索病毒的全球爆发”整个事件应该包括事件触发原因和事件影响扩散, 即宏观角度的安全事件 A 由单位安全事件 B、单位安全事件 C、单位安全事件 D 等其他关于触发原因和影响扩散的一系列单位安全事件的并集组成。

### 4.2　超网络演化模型构建方法

在真实世界的网络关系中, 通常是在已生成的超网络中, 新加入的一个节点和已有的若干个旧节点结合生成超边。例如, 在不同科学家进行合作的超网络中, 真实情况往往是加入的一个新科学家更偏向于和超网络中已经存在的若干数量的科学家合作; 顺利发表的一些新文章更倾向于引用一些已经被广泛引用过的经典文献。考虑到网络安全事件的文字关联特性以及超网络的独有特性, 结合 BA 无标度网络演化模型的构建思想[44], 现在给出一种基于安全事件的超网络演化模型构建方法。超网络演化模型构建算法如下[45]:

(1) 初始化: 假设初始时超网络有 $m_0$ 个节点 $v_1, v_2, \cdots, v_{m0}$, 每一个节点代表一个单位安全事件, 以及包含着 $m_0$ 个节点的一条超边 $E_1 = \{v_1, v_2, \cdots, v_{m0}\}$, 每一条超边代表单位安全事件之间存在的因果关系。

(2) 超边增长: 在 $t$ 时间内, 每次增加一个新的节点 $v$, 与 $m(m \leqslant m_0)$个已经存在的节点结合生成超边 $E_i = \{v_{i1}, v_{i2}, \cdots, v_{im}, v\}$。

(3) 优先连接: 从已有的超网络中的节点按照概率优先选取 $m$ 个节点, 与新加入的节点结合生成超边。每次选取连接的节点 $i$ 的概率 $\prod d_H(i)$ 等于节点 $i$ 的超度 $d_H(i)$与超网络中的已有节点 $j$ 的超度 $d_H(j)$ 总和之比, 即:

$$\prod d_H(i) = \frac{d_H(i)}{\sum_j d_H(j)} \tag{1}$$

其中 $d_H(i)$等于包含节点 $i$ 的超边的个数。经过 $t$ 时刻后, 超网络中有 $t$+1 条超边, $m_0$+$t$ 个节点, 所有节点的超度总和为 $m_0+t(m+1)$。

采用以上的增长和优先连接机制所产生的超网络模型, 由于每个时间步内生成一个新节点, 和网络中已有的 $m$ 个节点结合生成超边, 每条超边中的元素个数皆为 $m$+1, 所以得到的是($m$+1)均匀超网络模型。

## 5 基于安全事件演化模式框架的案例分析

2017 年的 5 月 12 日, 一种新型的勒索病毒, 即 WannaCry 利用“EternalBlue”(永恒之蓝)漏洞武器进行传播, 且传播力度非常猛烈。WannaCry 的大规模爆发, 使全球至少 150 个国家, 30 万名用户中招, 金融、能源、医疗等众多行业受到波及, 造成损失达 80 亿美元[46]。在我国内, 校园网成为重灾区, 大量实验室数据和毕业设计被锁定加密。另有部分大型企业的应用系统和数据库文件被加密后, 无法正常工作, 影响巨大[47]。

回顾整个勒索病毒的爆发过程, 我们不难发现 WannaCry 等蠕虫病毒只是勒索病毒大规模爆发的一个触发因素, 其根本原因是 Shadow Brokers(影子经纪人)黑客组织公开了由美国国家安全局掌控的漏洞武器: “永恒之蓝”。在 WannaCry 之前, 勒索病毒在较长时间内均为零散出现, 影响范围较小。当勒索病毒插上高危漏洞的翅膀, 便立刻掀起影响全球的蠕虫病毒风暴。与此同时, 跨地区、跨行业日益紧密的关联关系也是导致事件出现连锁并把影响扩大到全国大部分地区的重要原因。

由此, 本文将从影响扩散和发生原因两个角度建立勒索病毒的超网络连锁反应模型, 其建立过程为:

(1) 初始化: 将具体安全事件抽象为节点 $a$, $b$, $c$, $d$, $e$, $f$,…有限个节点。默认开始只存在节点 $a$, 以及包含着这个节点的 $n$ 条超边, $n$ 为自然数, 超边连接与 $a$ 存在直接因果关系的安全事件。

(2) 超边增长: 每次增加一个新的节点, 与 $a$ 节点结合生成新的超边。

(3) 优先连接: 从 $a$ 节点开始, 不断加入其他节点, 并从已有的超网络中的节点按照概率优先选取节点, 与新加入的节点结合生成超边。根据公式(1), 计算每次选中某个节点 $i$ 的概率, $i$ 可以是 $a,b,c,d,e,f,\cdots$ 中任意一个节点。最后可以得到每个节点的超边数量。

(4) 根据最终的节点和超边的数量, 得到事件层的关联关系, 并根据实际情况在超边中加入箭头表示因果关系, 同时在基础设施层加入实际基础设施、地域环境以及传播载体等不同的参数因素。

### 5.1 基于影响扩散的安全事件超网络模型

首先, 从 WannaCry 大规模爆发后影响不断扩散的角度建立模型。如图 4 所示, WannaCry 蠕虫病毒在全球的大规模爆发, 会直接导致五类安全事件的发生, 即高校等科研机构事件、政府机构事件、交通系统事件、公共服务系统事件和经济领域事件。

五类安全事件具体举例:

(1) 高校等科研机构事件: 截止 2017 年 5 月 14 日上午, 据我国教育网网络应急中心不完全统计, 全国近 1600 个教育网高校用户中有 66 个高校用户感染了 WannaCry 病毒, 致使很多实验数据及毕业设计被加密; 意大利米兰比科卡大学实验室大量实验室数据被锁定, 造成多项科研工作被强行停止。

(2) 政府机构事件: 全国多地公安业务系统受到 WannaCry 病毒影响, 导致对外的业务办理服务临时停止, 受影响的公安部门包括出入境、交管、户籍、人口管理和车管等; 俄罗斯政府发布消息, 内政部多个部门的电脑受到 WannaCry 病毒感染, 一度导致正常工作的停滞。

(3) 交通系统事件: 受交通道路系统感染 WannaCry 病毒的影响, 我国多处高速公路电子警示牌出现乱码等非正常显示的情况, 严重影响高速公路正常行车安全; 德国法兰克福机场一度因机场调度系统及行李存取系统感染病毒, 导致航班班次显示混乱, 行李大量堆积, 使得机场大量旅客滞留, 给航空业带来巨大压力。

(4) 公共服务系统事件: 德国慕尼黑公共停车服务系统被勒索病毒锁定; 沙特阿拉伯电信公司 STC 服务系统被锁定, 导致多项电信业务无法办理, 大量用户的个人信息存在泄露的危险[48]。

(5) 经济领域事件: 黑客通过 WannaCry 对重要文件和数据的锁定, 向用户勒索价值不等的财物, 直接经济损失近 10 亿美元; WannaCry 对比特币交易系统进行了攻击, 打乱了比特币正常的交易秩序, 对交易产生了严重的影响。

从安全事件层角度看, 五类安全事件之间存在连锁反应现象。高校等科研机构的数据资料等遭到锁定, 会影响科研工作向实际商业产品的转化, 商业产品的延期上市会造成一定的经济损失, 即导致其他领域发生安全事件; 公共服务系统事件, 诸如火车、公交汽车等公共交通的调度系统出现问题, 会

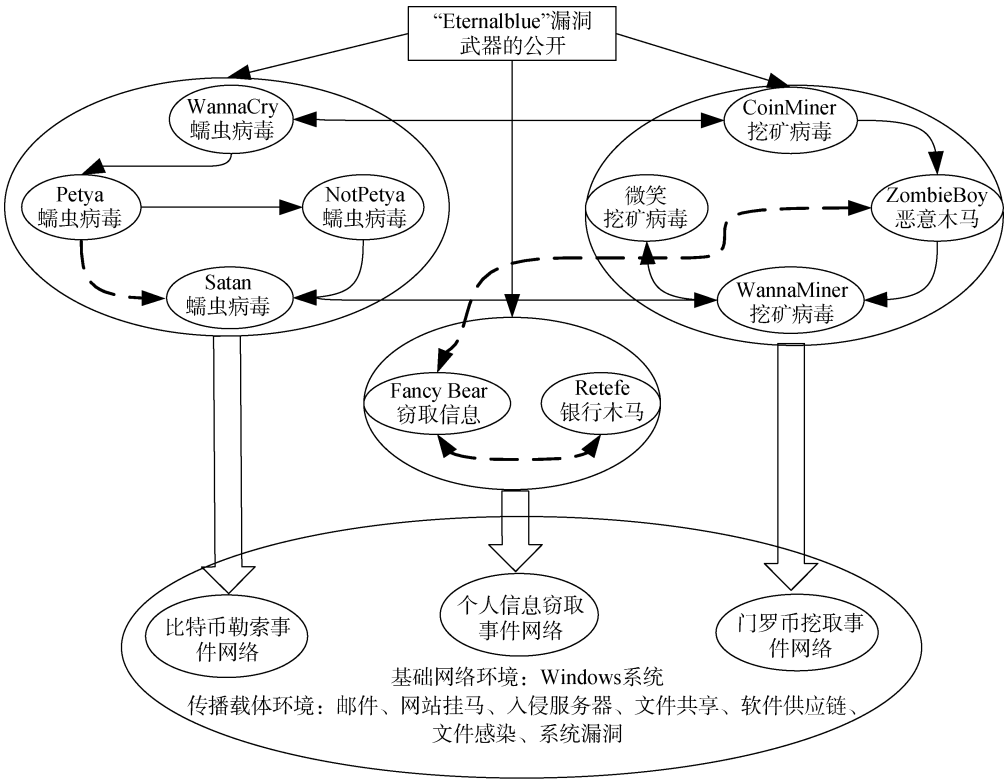



**图 4　基于触发原因的安全事件超网络模型**

**Figure 4　Super-network evolution model of security event based on triggering reason**

造成群众居民的出行受到影响, 即导致交通系统事件; 政府办事机构, 如公安、车管系统, 其电子办公系统受蠕虫病毒影响, 无法办理正常业务, 而其中很多业务与交通系统相关, 如驾驶执照的正常办理等; 交通系统事件的发生, 使物流运输受到影响, 物流受影响会导致已经成型的产品或原材料的运输问题, 进一步引起某些企业的经济损失。

在基础设施层, 每一类安全事件都有自己对应的基础设施, 即科研基础设施、政府办公设施、金融交易系统设施、交通基础设施和公共基础设施。基础设施是安全事件发生的环境基础, 更为具体的基础设施可以在超网络中抽象为环境节点。同时, 虽然这次 WannaCry 蠕虫病毒的爆发后影响已经扩散至全球, 但是规模和影响仍然存在一定的地域性分布。目标在国内主要影响范围在广东、浙江、北京、上海等经济发达省份, 国外的主要影响范围集中在吗, 美国、英国、德国、俄罗斯等发达国家。有这样的地域环境分布, 原因主要有两点:

(1) WannaCry 会通过锁定重要数据和资料来勒索用户的钱财, 经济实力的雄厚使发达地区成为攻击目标的可能性大大增加。

(2) WannaCry 蠕虫病毒主要通过网络进行传播, 众多互联网公司也是黑客的潜在攻击目标, 而这些公司一般来说都会将总部设置在经济发达地区。

## 5.2　基于触发原因的安全事件超网络模型

“永恒之蓝”(Eternalblue)漏洞的公开是勒索病毒的爆发和发展的主要原因, 因此以此漏洞为基础进行另一种安全事件超网络的模型的建立。如图 5 所示, 将“永恒之蓝”漏洞的典型利用事件分为了三大类, 即比特币勒索事件、个人信息窃取事件、门罗币挖取事件。比特币勒索事件包括 WannaCry 蠕虫病毒事件、Petya 蠕虫病毒事件、NotPetya 蠕虫病毒事件和 Satan 蠕虫病毒事件; 个人信息窃取事件包括 Fancy Bear 窃取信息事件和 Retefe 银行木马事件; 门罗币挖取事件包括 CoinMiner 挖矿病毒事件、ZombieBoy 恶意木马事件、WannaMiner 挖矿病毒事件和微笑挖矿病毒事件。

从安全事件层的角度看:

(1) 在比特币勒索事件网络中, 各事件均以“永恒之蓝”漏洞为触发原因, 形成按发生时间排序的安全事件连锁反应链, 即 WannaCry 蠕虫病毒→Petya 蠕虫病毒→NotPetya 蠕虫病毒→Satan 蠕虫病毒, 但同时 Petya 蠕虫病毒和 Satan 蠕虫病毒都是通过加密硬盘驱动器主文件表的方式进行比特币的勒索, 此处以虚线代表 Petya 蠕虫病毒事件有直接导致 Satan 蠕虫病毒事件发生的趋势。

(2) 在门罗币勒索事件网络中, 各事件均以“永恒之蓝”漏洞为触发原因, 形成按发生时间排序的安全事件连锁反应链, 即 CoinMiner 挖矿病毒→ZombieBoy 恶意木马→WannaMiner 挖矿病毒→微笑挖矿病毒。

(3) 在个人信息窃取网络中, Fancy Bear 是利用 APT 定向攻击旅店网络系统, 从而窃取旅店客人隐私信息, Retefe 银行木马攻击目标主要为瑞士、日本等国的银行, 进一步盗取用户银行信息。因为两者均与用户隐私信息有关, 此处用虚线表示两者有互相演化的趋势。

(4) 在三个不同安全事件网络之间, 也存在不同的连锁反应趋势。如 ZombieBoy 恶意木马在影响门罗币正常交易的同时, 也会通过远程后门窃取隐私信息, 与 Fancy Bear 有一定的转化趋势; WannaMiner 病毒和 Satan 病毒的主要攻击目标均为国内的企业用户; WannaCry 病毒和 CoinMiner 病毒对国内外未修复漏洞的的用户均选在巨大潜在的危害。

在基础设施层, 从触发原因的环境角度看, 整体的基础网络环境为 Windows 系统, 该病毒只攻击 Windows 系统的电脑, 几乎所有的 Windows 系统如果没有打补丁, 都会被攻击。如 Windows Vista、Windows Server 2008、Windows 7、Windows Server 2008 R2、Windows 8.1、Windows Server 2012、Windows Server 2012 R2、Windows Server 2016 等版本, 用户如果开启了自动更新或安装了对应的更新补丁, 可以抵御该病毒。Windows10 是最安全的, 由于其系统是默认开启自动更新的, 所以不会受该病毒影响。同时, Unix、Linux、Android 等操作系统, 也不会受到攻击[49]。

勒索病毒的具体传播方式也是基础设施层重要的因素, 随着勒索病毒发展日渐成熟, 其传播方式也变得趋于完善, 各家族勒索病毒传播方式也逐渐有了自身特点, 勒索病毒整体主要传播方式有以下几种:

(1) 邮件附件传播: 通过邮件附件进行传播的勒索病毒通常会伪装成用户常查看的文档, 如信用卡消费清单、产品订单等。附件中会隐藏恶意代码, 当用户打开后恶意代码便会开始执行, 释放病毒。

(2) 网站挂马传播: 网站挂马是在获取网站或者网站服务器的部分或全部权限后, 在网页中插入一段恶意代码, 这些恶意代码主要是一些 IE 等浏览器的漏洞利用代码。

(3) 入侵服务器: 针对服务器的攻击多通过暴力破解远程登录权限的方法。由于部分服务器未能及时修补安全漏洞, 以及普遍使用相同的密码或弱密码远程登录。不法黑客会用种种手段入侵企业服务器, 再手动卸载或关闭杀毒软件, 然后下载勒索病毒运行。

(4) 利用系统漏洞传播: 利用系统漏洞传播的特点是被动式中毒: 用户即使没有访问恶意站点, 没有打开病毒文件也会中招。利用系统漏洞传播的蠕虫病毒还会扫描同网络中存在漏洞的其他 PC 主机, 只要主机没有打上补丁, 就会被攻击。

(5) 网络共享文件: 一些小范围传播的敲诈勒索病毒会通过共享文件的方式进行传播, 不法黑客会将病毒上传到网络共享空间、云盘、QQ 群、BBS 论坛等, 以分享的方式发送给特定人群, 进而诱骗其下载安装。

(6) 软件供应链传播: 病毒制作者通过入侵软件开发、分发、升级服务等环节进行病毒传播。例如可以在产品组件中混入病毒, 或者当用户正常进行软件安装、升级时, 通过入侵劫持软件下载站和服务器, 勒索病毒可以趁虚而入。

(7) 文件感染传播: 利用感染型病毒的特点, 加密用户所有文档后再弹出勒索信息, 而由于 PE 类文件被感染后具有了感染其他文件的能力, 因此如果此文件被用户携带(U 盘、网络上传等)到其他电脑上运行, 就会使得该电脑的文件也被全部感染加密[50]。

## 6 讨论

本文旨在建立安全事件时空语义的关联关系模型, 揭示安全事件连锁反应机理, 为实现安全事件危害效用度量与评估方法提供理论基础, 丰富网络安全评估领域的研究。

为了解决上述问题, 本文从系统论的角度, 对安全事件点、链、网、超网络的四种演化模式进行递进式分析, 建立了基于超网络的网络安全事件连锁演化模型。

研究成果结合超网络的特点, 使网络安全事件内在的联系可以清晰的呈现出来, 从安全事件之间的关联关系入手, 有助于建立安全事件对网络系统安全程度的影响分析, 也有助于网络真实攻击和防御历史事件的分析以及攻防技术发展趋势分析。同时将超网络的研究领域进行了扩展, 从灾害到网络空间安全, 大大地丰富了超网络的应用范围。

但是目前还未形成自动化工具进行安全事件超网络分析, 还需人工参与; 还需进一步理论抽象, 使其应用于安全度量方面; 安全事件的评估还未能加入度量体系, 确立安全事件连锁相关的指标体系, 提出其量化分析方法是下一步的重点研究内容。

## 7 总结与展望

本文利用提出的安全事件演化模式框架, 从不同层次进行分析, 可以找到安全事件演化的真正原因, 发现安全事件爆发的隐患, 为有效应对安全事件危害的扩散提供决策依据。如果一个安全事件引发的演化模式属于安全事件超网络模式, 而仅从事件点、链或网的角度看待问题, 就可能忽视危害隐患, 导致危害扩大化; 反之, 如果一个突发事件发生后, 按照安全事件点、链、网、超网络的演化模式进行递进式分析, 并及时采取切断事件链或事件网的措施, 从而降低危害进一步扩散的风险。本研究旨在人们重视安全事件之间的多种关联的可能性, 在一个安全事件发生后, 应该从不同的角度发现引起连锁反应的可能性, 提前预警, 切断或尽量减少连锁反应的重要节点, 结合网络安全评估以降低安全事件的发生带来的损失。

**致　谢**　本课题得到国家重点研发计划“网络系统安全度量方法与指标体系”项目(No. 2016YFB0800700)资助。

## 参考文献

[1] Yang Yixian, Niu Xinzhen, and Li Mingxuan, “Network information security and confidentiality,” Beijing University of Posts and Telecommunications Press, 2001.
(杨义先, 钮心忻, 李名选, “网络信息安全与保密”, *北京邮电大学出版社, 2001*.)

[2] Which IT security tasks are you facing the most pressure to address?, https://www.statista.com/statistics/709789/most-pressing-global-cyber-security-issues/, Jan. 2018.

[3] The first anniversary of the outbreak of WannaCry, 5 million computers were attacked by ransomware, http://www.freebuf.com/articles/network/171608.html, May. 2018.
(在WannaCry爆发一周年之际, 500万台计算机遭到勒索软件攻击, http: //www.freebuf.com/articles/network/171608.html, May. 2018.)

[4] Eugene Schultz E. “Network Security Incident Response,” *Information Network Security*, no. 3, pp.35-35, 2003.
(EugeneSchultz E, “《网络安全事件响应》”, *信息网络安全, 2003* (*3*)*: 35-35*.)

[5] Gong Yu, Pei Xiaodong, Su Qi, and et al, “Survey of Network Security Situation Awareness,” Journal of Software, vol. 28, no. 4, pp.1010-1026, 2017.
(龚俭, 臧小东, 苏琪等, “网络安全态势感知综述”, *软件学报, 2017, 28*(*4*)*: 1010-1026*.)

[6] GB/Z 20986—2007 “Information Security Event Classification and Grading Guide”.
(GB / Z 20986—2007《信息安全事件分类分级指南》).

[7] System Theory, https://baike.baidu.com/item/%E7%B3%BB%E7%BB%9F%E8%AE%BA/1133820?fr=aladdin, Jun. 2018.
(系统论, https://baike.baidu.com/item/%E7%B3%BB%E7%BB%9F%E8%AE%BA/1133820?fr=aladdin, Jun. 2018.)

[8] Salah S, Maciá-Fernández G, and DíAz-Verdejo J S E. “A model-based survey of alert correlation techniques,” *Computer Networks*,vol. 57, no. 5, pp.1289-1317, 2013.

[9] Li Minggui, Xiao Yi, Chen Jianfeng, and et al, “Big Data-based Framework for Security Event Mining,” *Communications Technology*, vol. 48, no. 3, pp.346-350, Mar. 2015.
(李明桂, 肖毅, 陈剑锋等, “基于大数据的安全事件挖掘框架”, *通信技术, 2015, 48*(*3*)*:346-350*.)

[10] Zhong C, Yen J, Liu P, and et al, “Learning From Experts’ Experience: Toward Automated Cyber Security Data Triage,” *IEEE Systems Journal*, 2018.

[11] Cai Xiaozhi, Zhang Hexun, Xu Yang, and et al, “Management and technical points of life cycle management and control of security events,” *Network Security Technology and Application*, pp.16-16, 2018.
(蔡晓志, 张贺勋, 徐扬等, “安全事件生命周期管控管理及技术要点”, *网络安全技术与应用, 2018* (*3*)*: 16-16*.)

[12] Feng Tao, Zhang Yuqing, and Gao Youxing, “Network Security Incident Response Linkage System Model,” *Computer Engineering*, vol. 30, no. 13, pp.101-103, Jul. 2004.
(冯涛, 张玉清, 高有行, “网络安全事件应急响应联动系统模型”, *计算机工程, 2004, 30*(*13*)*:101-103*.)

[13] Wang Ruigang, “Research on Structure and Linkage of Nisier System,” *Computer Applications and Software*, vol. 28, no. 10, pp.117-119, Oct. 2018.
(王瑞刚, “网络与信息安全事件应急响应体系层次结构与联动研究”, *计算机应用与软件, 2011, 28*(*10*)*:117-119*.)

[14] Zhao Xu, Wen and Jiaxin Z, “Research on provincial network security emergency management platform based on secure access design,” *Research & Exploration in Laboratory*, vol. 37, no. 6, pp.293-296, Jun. 2018.
(赵旭, 文佳欣, Z, “基于安全访问设计的省级网络安全应急管理平台研究”, *Research & Exploration in Laboratory, 2018, 37*(*6*).)

[15] Wang Yingying, Luo Yi, Tu Guangyu, and et al. “Search Method for Power System Cascading Failures Using Graph Theory,” *High Voltage Engineering*, vol. 36, no. 2, pp.401-405, Feb. 2010.
(王英英, 罗毅, 涂光瑜等, “采用图论的电网连锁故障模式搜索方法”, *高电压技术, 2010, 36*(*2*)*:401-405*.)

[16] Zhai Plastic, Liu Youbo, Liu Junyong, and et al, “Cascading Failure Feature Analysis Based on Time-series Operation Evolution Model,” *Proceedings of the CSEE*, vol. 35, pp.82-92, Sep. 2015.
(刁塑, 刘友波, 刘俊勇等, “电力系统连锁故障的多层时序运行演化模型与应用”, *中国电机工程学报, 2015*(*S1*)*:82-92*.)

[17] Rong Lili, and Tan Hua, “Modelling Chain-reactions to Emergency Based on Disaster-pregnant Enviroment,” *Systems Engineering*, vol. 30, no. 7, pp.40-47, Jul. 2012.
(荣莉莉, 谭华, “基于孕灾环境的突发事件连锁反应模型”, *系统工程, 2012*(*7*)*:40-47*.)

[18] WANG Ning, LU Guo-Chen, and CHEN Ke, “Reasoning Method of Emergency Chain Reaction Path Based on Knowledge Element,” *Systems Engineering*, vol. 34, no. 5, pp.121-128, May. 2010.
(王宁, 路国粹, 钞柯, “基于知识元的突发事件连锁反应路径推理方法”, *系统工程, 2016*(*5*)*:121-128*.)

[19] Zhu Zhengwei, Zhao Xinxin, and Cai Li. “Simulation Study of Public Safety Emergencies Based on The Complex Dynamics Model of Emergency Proliferation,” *China Administration*, pp.125-128, 2012.
(朱正威, 赵欣欣, 蔡李, “突发公共安全事件扩散动力学模型仿真研究”, *中国行政管理, 2012*(*9*)*:125-128*.)

[20] Rong Lili, and Zhang Rong, “An emergency event chain reaction path deduction model based on discrete Hopfield neural network,” *Journal of Dalian University of Technology*, vol. 53, no. 4, pp. 607-614, Jul. 2013.
(荣莉莉, 张荣, “基于离散 Hopfield 神经网络的突发事件连锁反应路径推演模型”, *大连理工大学学报, 2013, 53*(*4*)*: 607-614*.)

[21] Katz G, Elovici Y, Shapira and B. CoBAn, “A context based model for data leakage prevention,” *Information Sciences*, vol. 262, no. 3, pp. 137-158, 2014.

[22] Dong J, “Impact of Bombardier Central ATS System Paralysis on Traffic Organization,” Urban Mass Transit, 2014.

[23] Moreno R, and Strbac G, “Integrating high impact low probability events in smart distribution network security standards through CVAR optimization,” Iet International Conference on Resilience of Transmission and Distribution Networks. IET, pp.1-6, 2016.

[24] Spanos G, and Angelis L, “The impact of information security events to the stock market,” Elsevier Advanced Technology Publications, 2016.

[25] Raven M C, Guzman D, Chen A H, and et al. “Out‐of‐Network Emergency Department Use among Managed Medicaid Beneficiaries,” *Health services research*, vol. 52, no. 6, pp. 2156-2174, 2017.

[26] Naheed M, Mahmood H, and Murtza I, “Secure multipath routing using link compromise metric in mobile ad hoc networks,” Electrical Engineering (RAEE), 2015 Symposium on Recent Advances in. IEEE, pp.1-5, 2015.

[27] Rong Lili, and Zhang Jiyong. “Research on different evolution models of emergency,” *Journal of Natural Disasters* vol. 21, no. 3, Jun. 2012.
(荣莉莉,, 张继永, “突发事件的不同演化模式研究”, *自然灾害学报, 2012*(*3*)*:03-06*.)

[28] National cybersecurity incident emergency plan, http://www.cac.gov.cn/2017-06/27/c_1121220113.htm, Sept. 2018.
(国家网络安全事件应急预案, http://www.cac.gov.cn/2017-06/27/c_1121220113.htm, Sept. 2018.)

[29] Su Jianfei, and Wang Jingwei, “Discussion on Network Security and Attack Techniques,” *Communications Technology*, vol. 43, no. 01, pp. 91-93, 2010.
(苏剑飞, 王景伟, “网络攻击技术与网络安全探析”, *通信技术, 2010* (*1*)*: 91-93*.)

[30] Ying Xiangrong. “The Importance of Active Defense System under the New Trend of Network Attack,” *Computer Security*, pp. 53-55, 2003.
(应向荣, “网络攻击新趋势下主动防御系统的重要性”, *计算机安全, 2003* (*29*)*: 53-55*.)

[31] Lin J, and Kang B, “Research on occurrence mechanism of public security emergency from the perspective of the structure box,” DEStech Transactions on Social Science, Education and Human Science, 2016.

[32] Qiu Jiangnan, Wang Yanzhang, and Zhang Rong, “A Model for Predicting Emergency Event Based on Bayesian Networks,” *Journal of Systems & M anagement*, vol. 20, no. 1, pp. 98-108, Feb. 2011.
(裘江南, 王延章, 董磊磊等, “基于贝叶斯网络的突发事件预测模型”, *系统管理学报, 2011, 20*(*1*)*: 98-103*.)

[33] Perrig A, and Stankovic J, “Wagner D. Security in wireless sensor networks,” *Communications of the ACM*, vol. 47, no. 6, pp. 53-57, 2004.

[34] Gan G, Lu Z, and Jiang J, “Internet of things security analysis,” Internet Technology and Applications (iTAP), 2011 International Conference on. IEEE, pp.1-4, 2011.

[35] Ma Tao, and Guo Jinli, “Forming mechanism of matrix system enterprise project team hypernetwork based on hypergraph,” *Application Research of Computers*, vol. 35, no. 1, Jan. 2018.
(马涛, 郭进利, “基于超图的矩阵制企业项目小组超网络形成机制研究”, *计算机应用研究, 2018, 1: 015*.)

[36] Q Zhu, and AT Azar, “Complex system modelling and control through intelligent soft computations,” Germany: Springer, 2015.

[37] Li Y X, and Xie Y J, “Analysis and enlightenment on the cybersecurity strategy of various countries in the world,” *Chinese Journal of Network and Information Security*, vol. 2, no. 1, pp. 1-5, 2016.

[38] Wang Zhongtuo, and Wang Zhiping, “Elementary Study of Supernetworks,” *Chinese Journal of Management*, vol. 5, no. 1, Jan. 2008.
(王众托,, 王志平, “超网络初探”, *管理学报, 2008, 5(1): 1*.)

[39] Daskin M S, “Urban transportation networks: Equilibrium analysis with mathematical programming methods,” 1985.

[40] Nagurney A, Dong J, “Supernetworks: decision-making for the information age,” Elgar, Edward Publishing, Incorporated, 2002.

[41] Fu-li S, Yong-lin L, and Yi-fan Z, “A military communication supernetwork structure model for netcentric environment,” Computational and Information Sciences (ICCIS), 2010 International Conference on. IEEE, pp. 33-36, 2010.

[42] Super network, https://baike.baidu.com/item/%E8%B6%85%E7%BD%91%E7%BB%9C/6663430?fr=aladdin, Nov. 2014.
(超网络, https://baike.baidu.com/item/%E8%B6%85%E7%BD%91%E7%BB%9C/6663430?fr=aladdin, Nov. 2014.)

[43] Elementary event, https://baike.baidu.com/item/%E5%9F%BA%E6%9C%AC%E4%BA%8B%E4%BB%B6/552306?fr=aladdin, June. 2018.
(基本事件, https://baike.baidu.com/item/%E5%9F%BA%E6%9C%AC%E4%BA%8B%E4%BB%B6/552306?fr=aladdin, June. 2018.)

[44] Zhou Q, Chen J, Liu H, et al, “Simulation Software for Evolution of BA Scale-free Networks Based on LabVIEW,” Electronic Sci-

ence & Technology, 2016.

[45] Hu Feng, Zhao Haixing, and Ma Xiujuan, "An evolving hypernetwork model and its propertiesl," *Science in China: Physics Mechanics Astronomy*, vol. 43, no. 1, pp. 16-22, Jan. 2013.
(胡枫, 赵海兴, 马秀娟, "一种超网络演化模型构建及特性分析", *中国科学: 物理学 力学 天文学, 2013(1):16-22*.)

[46] Tengxu computer housekeeper. WannaCry worm first anniversary, blackmail virus, http://www.freebuf.com/articles/system/ 171448.html, May. 2018.
(WannaCry 蠕虫一周年, 勒索病毒狼烟四起, http://www.freebuf.com/articles/system/171448.html, May. 2018.)

[47] Kirin. WannaCry ransomware, this is the case, https://www.guokr.com/article/442167/, May.2017.
(麒麟.WannaCry 勒索病毒, 是这么一回事, https://www.guokr.com/article/442167/, May.2017.)

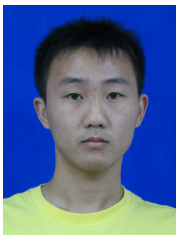
[48] Scenes infected by WannaCry virus attack, http://www.freebuf.com/news/135095.html, May. 2017.
(那些被 WannaCry 病毒攻击感染的场景, http://www.freebuf.com/news/135095.html, May. 2017.)

[49] Pascariu C, BARBU I D, Bacivarov I C. Investigative Analysis and Technical Overview of Ransomware Based Attacks. Case Study: WannaCry. *Int'l J. Info. Sec. & Cybercrime*, 2017, 6: 57.

[50] Deep technical analysis of ransomware WannaCry - detailing the details of transmission, infection and hazards, https://www.secpulse.com/archives/58077.html, May. 2017.
(勒索病毒 WannaCry 深度技术分析——详解传播、感染和危害细节,https://www.secpulse.com/ archives/58077.html, May. 2017.)

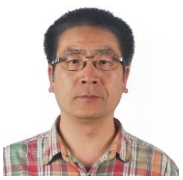
**姬逸潇** 于 2016 年在燕山大学信息安全专业获得学士学位。现在西安电子科技大学密码学专业攻读硕士学位。研究领域为网络安全态势感知、网络系统安全评估。研究兴趣包括: 云计算安全、大数据安全等。Email: jiyx@nipc.org.cn。

**吴晨思** 于 2013 年在中北大学软件工程专业获得学士学位。现在中国科学院大学信息安全专业攻读博士学位。研究领域为网络安全与评估。研究兴趣包括: 大数据安全、安全漏洞。Email: wucs@nipc.org.cn。



**杨粟** 于 2016 年在电子科技大学信息安全专业获得学士学位。现在中国科学院大学信息安全专业攻读博士学位。研究领域为信息安全与机器学习、网络评估。研究兴趣包括: 物联网安全、大数据安全等。Email: yangs@nipc.org.cn。

**郭敏** 于 2016 年在吉林大学获得应用数学专业硕士学位。北京计算机技术及应用研究所工程师, 研究领域为网络安全。研究兴趣包括: 数据安全、数据挖掘等。Email: guominjmh@163.com。



**张玉清** 于 2000 年在西安电子科技大学密码学专业获得博士学位。现任国家计算机网络入侵防范中心主任。研究领域为漏洞挖掘、系统安全。研究兴趣包括: 物联网安全、大数据安全、安全评估等。Email: yangs@nipc.org.cn。