跨境网络攻击治理及中国方案

梁思雨[1] 孔华锋[2*]
[1](公安部第三研究所 上海 201204)
[2](武汉商学院 武汉 430056)

摘 要 当前跨境网络攻击行为呈现多发高发态势,面向关键信息基础设施发起的攻击直接威胁一国网络主权,动摇国家安全和社会稳定基石。如何提高和运用本国网络防御及威慑能力,妥善处理行为者归因、跨境证据调取等问题成为跨境网络攻击治理过程中亟待解决的难题。面对新形势下跨境网络攻击在主体、对象、路径方面的新特点,美国持续通过战略立法和国际合作完善其综合治理体系。我国在维护网络主权的基本原则上,需转变网络安全保障理念,落实现有制度规定,并通过拓展国际合作,充分保障我国网络空间主权、安全和发展利益。

关键词 跨境网络攻击 关键信息基础设施 网络安全法

中图分类号 TP3 **文献标识码** A DOI:10.3969/j.issn.1000-386x.2019.12.049

THE GOVERNANCE OF CROSS-BORDER CYBER ATTACK AND CHINESE SOLUTION

Liang Siyu[1] Kong Huafeng[2*]
[1](*The Third Reasearch Institute of the Ministry of Public Security, Shanghai 201204, China*)
[2](*Wuhan Business University, Wuhan 430056, Hubei, China*)

Abstract The cross-border cyber-attacks have appeared to be in a trend of frequent occurrence and high incidence, and attacks directed at critical information infrastructure directly threaten a country's cyber sovereignty and shake the cornerstone of national security and social stability. How to improve and apply the domestic cyber defense and deterrence ability, and properly handle the attribution of actors and cross-border evidence acquisition, has become an urgent problem to be solved in the process of cross-border cyber-attack governance. Facing the new characteristics of cross-border cyber-attack in terms of subject, object and path under the new era, the United States continues to improve its comprehensive governance system through strategic legislation and international cooperation. Under the basic principles of safeguarding cyber sovereignty, China needs to change the concept of cybersecurity assurance, implement the existing institutional regulations, and fully safeguard the interest of China's cyberspace sovereignty, security and development through expanding international cooperation.

Keywords Cross-border cyber-attack Critical information infrastructure Cybersecurity law

0 引 言

当前,网络攻击和关键信息基础设施损害作为技术类风险,都已列入全球影响力最大的十大风险[1]。而面向关键信息基础设施的跨境网络攻击更是上升到国家和社会安全层面,直接威胁一国网络主权。军事国防已经成为全球 APT 攻击的首要目标[2],包括政府部门、委内瑞拉水电站及乌克兰电网在内的能源、交通、金融、医疗行业等关键信息基础设施领域都曾遭受网络攻击。2017 年爆发的 WannaCry 勒索病毒事件更是直接波及全球 150 多个国家和地区,造成大量基础

收稿日期:2019-04-11。国家重点研发计划项目(2018YFC0830401);公安部第三研究所 2019 年基本科研业务费专项资金项目(C19201);上海市 2017 年度"科技创新行动计划"高新技术领域项目(17DZ1101004);公安部第三研究所 2018 年基本科研业务费专项资金项目(C18355)。**梁思雨**,研究实习员,主研领域:网络安全法。**孔华锋**,教授。

设施停摆。因此,面向关键信息基础设施的跨境网络攻击高发态势要求各国亟需建立健全相应治理体系。

鉴于跨境网络攻击已成为全球需共同面对和解决的难题,美国作为传统网络强国,持续通过战略立法和国际合作加紧布局,逐步建立防御与威慑并重的治理体系。我国作为网络大国也难以独善其身,《国家安全法》首次确立网络主权原则,并通过《网络安全法》《反恐怖主义法》《国际刑事司法协助法》逐渐建立起面向关键信息基础设施的跨境网络攻击治理体系。然而,由于此种攻击多暗含地缘政治因素,在追踪溯源、证据调取和司法协助等方面仍然面临困境,使得单凭一国难以达到应有效能。我国需在借鉴国外经验的基础上,通过转变安全观、落实现有立法、推动国际合作等途径,建立面向关键信息基础设施的跨境网络攻击综合治理体系。

1 新形势下跨境网络攻击治理困境

当前国际社会对于网络攻击或跨境网络攻击尚未形成统一概念。《塔林手册 2.0 版》中将“网络攻击”定义为无论进攻还是防御,可以合理预见导致人员伤亡或物体损害的网络行动[3]。我国指导性技术文件《信息安全技术信息安全事件分类分级指南》(GB/Z 20986 - 2007)中将“网络攻击事件”定义为通过网络或其他技术手段,利用信息系统缺陷或暴力实施攻击,并造成信息系统异常或潜在危害的信息安全事件(包括拒绝服务攻击、后门攻击、漏洞攻击等)。可见,网络攻击的本质只是一种行为,发现目标系统的脆弱性,并创建一个包含恶意软件的工具来利用此漏洞[4],从而影响目标系统正常运行。跨境网络攻击的特殊性体现在攻击行为来源于境外,常涉及多个国家或地区的基础设施、网络及人员,单纯依靠本国国内法难以有效规制,需要在立法和实践方面与国际接轨。

网络能力在和平时期、国际关系紧张时期以及武装冲突时期都可以使用,并且现阶段国家和非国家行为者都掌握了此种能力,使得对于跨境网络攻击的治理形势更加严峻。首先,攻击主体更加精细,目的趋于政治化。网络行为者脱离单兵作战,开始形成结构复杂、分工明确、来源广泛的有组织、规模化团体。从乌克兰电网事件、“震网”病毒事件等看出跨境网络攻击已具有政治化倾向,攻击目的从单纯窃取、诈骗等非法占有目的,转变为国际竞争与博弈的有力工具。其次,攻击对象向关键信息基础设施领域渗透。与政治化倾向相伴而生的是攻击对象的转移。鉴于网络与社会基础运营领域的深度融合,关键信息基础设施对国家安全和社会长治久安的影响程度持续加深,通过打击关键信息基础设施,可以更加直接了当地彰显网络威慑能力。最后,攻击门槛持续降低,路径更加复杂。围绕网络违法犯罪行为形成的黑灰产业链日益庞大且分工精细,从组织者到程序开发、分发、攻击入侵和事后贩卖活动都囊括在内。简单易学的攻击方法、泛滥成灾的工具交易使得发起跨境网络攻击的门槛持续降低,加重非对称性。同时,随着物联网、区块链等新一代信息技术的发展以及虚拟货币的兴起,行为者在攻击活动中更易隐藏其行为痕迹,跨境网络攻击更具隐蔽性,行为者溯源归因更加复杂。

面对持续严峻的跨境网络攻击态势,各国纷纷在技术和立法方面加紧布局。美国、欧盟、俄罗斯、我国等国家和地区皆通过战略立法、实践等途径加强跨境网络攻击治理。鉴于新形势下跨境网络攻击在主体、对象和路径方面的新特点,使该问题的治理已经超出一国范畴,成为国际社会共同面临的难题。

受限于各国立法水平参差不齐,以及不同利益博弈和社会背景,短时间内未达成国际通行的实体和程序法规定,使得各国在归因、证据调取、电子数据取证等方面面临管辖权和国际间协助执法的问题。《塔林手册 2.0 版》明确在国家法的限制范围内,国家可对网络活动行使属地和域外管辖权,而国家法理论中,针对跨境网络攻击,受害国行使的是保护性管辖,但这种管辖权获取的前提也要求达到一定的危害程度。然而在实践中,对于危害程度并没有统一的量化标准,使各国在行使管辖权时主观性较大,易造成国家力量控制责任追究的局面。

因此,在通过战略立法、技术创新、人才培养等途径强化本国抵御跨境网络攻击的同时,也需要通过国际合作,妥善解决在行为者归因、跨境证据调取、引渡、驱逐或国外起诉等方面存在的争议。

2 美国跨境网络攻击之治理措施

目前,美国主要从区分保护,强调关键基础设施保护,加强惩戒措施,提高潜在威慑力以及拓展国际合作广度与深度,形成统一联盟三方面治理跨境网络攻击,试图建立牢固的跨境网络攻击抵御防线。

2.1 美国跨境网络攻击治理现状

美国作为网络领域的传统强国,在跨境网络攻击应对方面也早有布局,从战略、立法和实践多方面共同入手,提高本国跨境网络攻击防御和威慑能力。

2.1.1 发布战略,夯实国家顶层设计

美国先后发布《网络空间国际战略》《网络战略》

《国家网络战略》等战略文本,夯实跨境网络攻击治理的顶层设计。

2011 年,美国首次发布全面的《网络空间国际战略》(International Strategy for Cyberspace)[5]。该战略阐述了美国对网络发展的愿景,并制定了与其他国家合作共同实现这一愿景的议程。在治理恶意网络活动方面,战略指出美国将拓展更广泛的合作关系,深化在执法和法治方面的合作,扩大《网络犯罪公约》共识范围,协调网络犯罪国际立法,从而阻止和威慑恶意网络活动行为者。如有必要,美国将在国际法框架下,对网络空间的敌对行为作出回应,并保留使用一切必要手段的权利。此外,美国将建立和加强现有的军事联盟,以提高集体安全。

在国防部 2015 年发布的《网络战略》(Cyber Strategy)中,首次明确讨论了在何种情况下,可以使用网络武器打击攻击行为者[6]。2018 年 9 月,国防部发布新版《网络战略》[7],取代 2015 年发布的版本。新版本下的战略从确保包括网络空间在内的军事实力,打击可能导致重大网络事件的针对关键基础设施的恶意网络活动以及加强国际合作,增强双向信息共享三方面维持美国在网络空间的战略优势。在阻止恶意网络活动方面,战略指出美国将利用所有的国家权力工具保护美国国家利益、盟友和合作伙伴免受恶意网络活动威胁。如果威慑不足以达到效果,联合军队将时刻准备利用各种军事能力以作回应。

同月,白宫发布 15 年来首份国家层级的《国家网络战略》(Naitonal Cyber Strategy)。该战略建立在 2017 年《增强联邦政府网络与关键性基础设施网络安全总统行政令》(13800)行政命令基础上,围绕维护美国利益、促进美国繁荣、维护和平、增强美国影响力四方面展开。在跨境协助方面,美国将在合法引渡、消解协调障碍、鼓励以执法为目的进行有效跨境信息交流方面开展工作,并有效利用和扩大现有《网络犯罪公约》等国际共识。

美国将在国际法基础上促进建立网络空间中负责任的国家行为框架,遵守和平时期适用的自愿不具约束力的国家行为规范,并考虑采取切实可行的信任措施以减少冲突风险。美国明确包括外交、信息、军事、财务、情报在内的所有国家权力工具都可用于预防、应对和阻止针对美国的恶意网络活动,将正式并定期展开国际合作,通过综合战略识别、归因和阻止恶意网络活动,并在适当时刻对威胁国家利益的恶意网络行为者施加后果。此外,美国还将发布一项国际网络威胁倡议,建立联盟并制定战略,确保对手了解其恶意网络行为的后果,协调和支持彼此对重大恶意网络事件的反应,包括情报共享、支持归因声明、支持采取响应行动的公开声明、以及对恶意行为者共同施以后果。

2.1.2　完善立法,建立综合治理体系

在具体的立法和命令层面,奥巴马和特朗普执政期间都致力于通过完善认定标准、完善电子数据取证、强化威慑能力和加强国际合作等,从实体和程序两方面治理跨境网络攻击。

行政命令层面,2015 年,奥巴马通过签署行政命令[8],赋予美国政府制裁跨境网络攻击行为者的权力。明确当境外网络活动对美国国家安全、外交政策、经济稳定造成重大威胁,美国政府可以冻结行为者的资产,并且暂停其作为移民或非移民身份进入美国。

2016 年 7 月,奥巴马发布关于网络事件协调的总统政策指令(PPD-41)[9],明确政府应对网络事件的原则和具体内容,是联邦政府应对重大网络事件的重要里程碑式文件。PPD-41 意义在于对网络事件和重大网络事件进行划分,并明确相应标准,为后续政府行动提供依据。PPD-41 将“重大网络事件”定义为可能对国家安全利益、外交关系、经济稳定、公众信心、公民自由、公共健康和公民安全造成显著损害的网络事件。在应对所有网络事件时,联邦政府将在共同责任、基于风险、尊重受影响实体、协调政府行动及应急恢复原则的基础上,同时开展威胁响应、资产响应和情报支持等相关活动。对于重大网络事件,政府将在国家政策、机构职责协同和地域配置方面展开,通过协调政策和战略的制定实施、明确联邦牵头机构等方式有效应对重大网络事件。与此同时,联邦政府发布了用于描述网络事件严重程度的通用模型[10],从国家安全角度讲网络事件分为 0 到 5 六个级别,3 级及以上的网络事件为“重大事件”,将触发 PPD-41 中协调机制的应用。

特朗普执政期间,2018 年 11 月,特朗普签署《网络安全与基础设施安全机构法 2018》,将国土安全部下“国家保护和规划局”更名为“网络安全和基础设施安全局”,承担关键基础设施保护、网络安全和其他相关工作。对美国关键基础设施和核心资源漏洞进行全面评估,包括美国境内特定类型恐怖袭击所构成的风险,袭击成功的可能性以及应对措施的可行性及效力。并且制定一项包括信息技术和电信系统在内的国家关键基础设施和核心资源综合性国家计划,加强合作,改善信息共享。

2019 年 2 月,参议院提出《保护美国安全,免受克里姆林宫侵略法案 2019》。在一般计算机相关欺诈活动刑罚的基础上,加重对关键基础设施领域计算机造成损害的惩处力度。通过将监禁期限延长至不超过 20 年,且不得缓刑,强化关键基础设施保护。

2018 年 12 月,美国参议院提出一项决议,督促建立印度-太平洋地区网络联盟以应对网络威胁。决议要求建立印度-太平洋地区网络联盟(CLIPS),成立信息共享分析中心,以建立全天候网络威胁监测和缓解机制。此外,联盟国间还应引渡网络窃贼,在跨境网络攻击的溯源和反制方面展开合作,以威慑潜在攻击行为者。

此外,在程序法方面,2016 年美国通过《41 号修订案》,对《联邦刑事诉讼法》进行修订。修订案明确任何可能与网络犯罪相关的地区法官都有权发布授权令,赋予联邦执法机构通过远程访问工具访问位于法院管辖区之外的计算机的权限。这使得 FBI 在调查跨境网络攻击时拥有更广泛的域外权限,极大增强美国在此方面的调查能力。

2.1.3 拓展合作,深化现有国际共识

在《网络空间国际战略》的指引下,美国积极在立法和实践中加强国际合作,致力于达成更大范围的共识。2015 年 9 月,中美就网络问题达成承诺[11]:两国政府同意合作并及时回应有关其领土内发生的恶意网络活动的信息和协助请求;不会为了商业利益而进行或故意支持通过网络盗窃知识产权;两国政府共同努力,进一步确定和推广适当的网络空间国家行为规范,并在网络空间成立国际安全问题高级专家组;并且建立起打击网络犯罪及相关问题的部长级联合对话机制。

同年 11 月,二十国集团领导人发表声明,确认国际法,特别是《联合国宪章》,应适用于国家在信息通信技术方面的行为,并承诺所有国家都应遵守负责任的国家规范。任何国家都不应出于获取商业竞争优势的目的,进行或支持通过信息通信技术窃取知识产权,包括商业秘密或其他商业机密信息。声明还强调了联合国在制定规范方面发挥的关键作用。

2.2 美国跨境网络攻击治理特点分析

在跨境网络攻击治理过程中,美国认识到其在应对构成使用武力水平的跨境网络攻击时处于有利地位,但面对低于使用武力阈值,大量增加的由国家支持的跨境网络攻击,仍面临一定挑战[12]。单纯的被动防御不足以阻止国家支持的恶意行为者,需要采取其他措施增强美国的网络威慑能力。由此,美国从单纯的被动防御逐渐走向威慑与防御并重的理念,侧重彰显本国网络实力,重视对潜在恶意网络行为者的威慑作用,从而确保美国在应对跨境网络攻击中处于优势地位。

2.2.1 区分重点,强调关键基础设施保护

美国一直将维持和提升网络系统面对跨境网络攻击时的复原力作为政策重点,其中关键基础设施的安全保障更是重中之重。通过设立专门部门,对关键基础设施和核心资源漏洞进行全面评估,制定综合性国家计划等手段加强前期保护,通过加重对关键基础设施造成损害的惩处力度,重视事后惩处。

2.2.2 严厉惩戒,重视潜在网络威慑能力

通过行政命令和立法,美国逐步建立起政府对跨境网络攻击施以制裁的权力体系及内容。面对跨境网络攻击行为者,美国有权冻结其资产,并综合运用多种手段,包括限制行为者入境。当前,美国政府正试图通过立法要求识别国家支持的网络活动中的核心威胁主体,并施以制裁。

在网络威慑能力方面,美国多次强调面对跨境网络攻击高发趋势,包括经济、军事、外交、情报在内的国家工具都应纳入必要的治理手段。并且强调在必要情况下,对网络空间敌对行为作出回应,并保留相应手段的权利。如果单纯威慑不足以达到应有效果,美国将时刻准备利用各种军事能力以作回应。

2.2.3 加强合作,形成共同应对联盟

美国政府充分认识到扩大国际共识,在国际社会寻求最大程度的合作对于应对跨境网络攻击不可或缺。当前《联合国宪章》《网络犯罪公约》可延展适用于跨境网络攻击治理,并且二十国集团承诺国际法同样适用于网络空间行为,但各国立法和实践能力不同,使得跨境治理在归因、证据调取、引渡、国外起诉、协助执法方面仍面临困境。

因此,美国在战略、立法和实践中,反复强调加强国际合作的现实紧迫性,并通过发起网络威胁国际倡议、加强国家间信息共享、达成国家或地区间承诺等方式,形成共同应对跨境网络攻击的合作机制。

3 跨境网络攻击治理之中国方案

目前,我国没有针对跨境网络攻击的专门立法,零星分布在《国家安全法》《网络安全法》《反恐怖主义法》《国际刑事司法协助法》等相关立法中。

3.1 跨境网络攻击治理的现有措施

我国现有立法在跨境网络攻击治理的实体和程序法方面都有所涉及,在明确法律责任的同时,确保其依法有效落实。《国家安全法》首次在立法层面确立网络主权原则,《网安法》作为网络空间基础性法律,进一步明确我国维护网络主权的态度,要求采取措施,监测、防御、处置来源于境内外的网络安全风险和威胁,保护关键信息基础设施免受攻击、侵入、干扰和破坏。

为实现这一目的,《网安法》第 75 条明确法律责任,对于境外主体攻击、侵入、干扰和破坏我国关键信息基础设施,并造成严重后果的,我国公安和有关部门有权追究其法律责任,可以决定对该行为者采取冻结财产或者其他必要制裁措施。《反恐怖主义法》第 11 条规定对在我国领域外对我国国家、公民或者机构实施的恐怖活动犯罪,或者实施我国缔结、参加的国际条约所规定的恐怖活动犯罪,我国将行使刑事管辖权,依法追究刑事责任。跨境网络攻击在特定情形下也可构成恐怖主义行为,从而触发我国刑事管辖权。

程序法方面,《刑事诉讼法》将电子数据纳入证据范畴,行政机关在行政执法和查办案件过程中收集的电子数据,可以在刑事诉讼中作为证据使用。为提高电子数据证据价值,“两高一部”接连发布《关于办理网络犯罪案件适用刑事诉讼程序若干问题的意见》和《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》,明确当原始存储介质位于境外,无法获取时,可以提取电子数据。对于原始存储介质位于境外或者远程计算机信息系统上的电子数据,可以通过网络在线提取,赋予我国侦查机关在调查跨境网络攻击时在线提取境外电子数据的权力。在国际司法协助方面,2018 年 10 月我国通过《国际刑事司法协助法》,就刑事司法协助的调查取证、涉案财物处理、以及被判刑人移管方面进行规定,为我国在调查跨境网络攻击时对外提出司法协助请求,以及妥善处理他国请求时提供指引。

3.2　跨境网络攻击治理的中国方案

虽然我国立法已有所规定,但跨境网络攻击的治理是一项系统工程[12],其复杂性远超于现有立法的有效适用,需要在立足我国实践的基础上,吸收国外先进经验,全面提升我国网络攻击应对的有效性。

3.2.1　风险防范前置,转变理念

当前,跨境网络攻击手段和路径日益复杂,工具日趋多样,加之网络事件后果的破坏性和不可逆性,我国需打破传统攻防理念,从单纯的被动防御逐步转向综合的积极防御理念,从强调惩治转向关注风险的前期预防和消解。《网安法》要求建立网络安全监测预警和信息通报制度,国家网信部门协调建立健全风险评估和应急工作机制。说明我国在顶层设计层面已经逐渐意识到积极防御的现实需求。在后续落地过程中,需切实落实相关制度,建立协调机制,确保在网络风险增大时及时控制消解潜在威胁,网络安全事件发生后最大程度减缓损失。此外,通过应急演练等方式,适时适当展示我国网络实力,提升网络威慑能力。

3.2.2　落实现有立法规定,推动共识

我国现有立法在实体和程序上为跨境网络攻击治理奠定了基础,后续制度落地和提高立法实用性成为需重点关注的方面。基于网络本身的技术性和特殊性,要求用好《网安法》75 条和《国际刑事司法协助法》等规定,妥善处理跨境网络攻击法律责任、证据调取和司法协助方面的问题。

此外,我国应在《网络空间国际合作战略》引导下,在跨境网络攻击应对层面扩大共识,改善国家间威胁情报共享,技术和策略上互通有无,对于诸如危害程度等需要量化的标准尽早达成可普遍适用的标准。

3.2.3　夯实安全保障底层架构,落实基础

重视技术的自主可控。当前国际局势紧张,我国在大数据、云计算、物联网、人工智能的新兴技术领域需提前布局,实现核心技术的突破,重视核心技术的自主可控,避免受制于人,陷入被动局面。同时,将网络安全需求嵌入技术、产品的全生命周期。

强调人才培养的重要性。在美国的战略立法中都将网络安全人才培养放在关键位置,将其从小学贯彻至高等教育,通过开展职业或专项教育,成立专门的网络队伍等方式培养专业人才。2017 年,中央网信办和教育部公布我国首批“一流网络安全学院”,逐步开展我国网络安全人才培养工作。在此基础上,我国需在全社会培育网络安全文化,综合运用学科教育、职业教育、漏洞悬赏计划、技能大赛等多种方式,充分调动社会主体参与人才培养的积极性。

4　结　语

网络主权是一国主权在网络空间的延伸,我国通过《国家安全法》《网络安全法》确立维护网络主权的基本原则。面向关键信息基础设施的跨境网络攻击将直接对网络主权构成冲击,要求我国充分运用各种国家工具建立健全跨境网络攻击治理体系。当前,跨境网络攻击主体更加精细化,对象逐渐向关键信息基础设施领域渗透,并且攻击门槛持续降低,路径更具隐蔽性,使得跨境网络攻击治理面临新的困境。与此同时,美国转变理念,网络防御和威慑能力并重,通过加强关键基础设施保护、赋予联邦执法机构更加广泛的调查权限、加强国际合作推动共识等手段,维持本国在治理跨境网络攻击方面的优势地位。我国虽已赋予有关部门实体和程序性权力,仍需在网络安全保障理念、落实现有立法规定、夯实技术创新和人才培养等安全保障基础架构以及国际合作方面加以完善,以遏制跨境网络攻击高发态势,维护我国网络空间主权、安全和发展利益。

参 考 文 献

[1] World Economic Forum. The global risks report 2019 14th edition[DB/OL]. 2019 - 01 - 06[2019 - 04 - 09]. http://www3. weforum. org/docs/WEF _ Global _ Risks _ Report _ 2019. pdf.

[2] 360 互联网安全中心. 全球高级持续性威胁(APT)2018 年总结报告[DB/OL]. 2019 - 01 - 11[2019 - 04 - 10]. http://zt. 360. cn/1101061855. php? dtid = 1101062514&did = 210827151.

[3] 迈克尔·施密特. 网络行动国际法:塔林手册 2. 0 版[M]. 黄志雄,译. 北京:社会科学文献出版社,2017:92.

[4] Libicki M C. Cyberspace is not a warfighting domain[J]. Journal of Law and Policy for the Information Society, 2012. 8(2): 328 - 335.

[5] Schmidt H A. Launching the U. S. international strategy for cyberspace [DB/OL]. 2011 - 05 - 16[2019 - 03 - 31]. https://obamawhitehouse. archives. gov/blog/2011/05/16/launching-us-international-strategy-cyberspace.

[6] 方兴东,陈帅. 辨析美国网络安全战略的错误抉择——从勒索病毒反思美国网络安全战略[J]. 汕头大学学报(人文社会科学版),2017,33(5):12 - 19.

[7] Summary: department of defense cyber strategy 2018 [DB/OL]. 2018 - 09 - 18[2019 - 03 - 28]. https://media. defense. gov/2018/Sep/18/2002041658/ - 1/ - 1/1/CYBER_STRATEGY_SUMMARY_FINAL. PDF.

[8] Executive Order— "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities" [DB/OL]. 2015 - 04 - 01[2019 - 03 - 31]. https://obamawhitehouse. archives. gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m.

[9] Presidential Policy Directive—United States Cyber Incident Coordination [DB/OL]. 2016 - 07 - 26[2019 - 03 - 31]. https://obamawhitehouse. archives. gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

[10] FACT SHEET: Presidential Policy Directive on United States Cyber Incident Coordination [DB/OL]. 2016 - 07 - 26 [2019 - 03 - 31]. https://obamawhitehouse. archives. gov/the-press-office/2016/07/26/fact-sheet-presidential-policy-directive-united-states-cyber-incident-1.

[11] Christopher Painter. International Cybersecurity Strategy: Deterring Foreign Threats and Building Global Cyber Norms [DB/OL]. 2016 - 05 - 25[2019 - 03 - 31]. https://2009 - 2017. state. gov/s/cyberissues/releasesandremarks/257719. htm.

[12] Office of the coordinator for cyber issues. Recommendations to the president on deterring adversaries and better protecting the American people from cyber threats [DB/OL]. 2018 - 05 - 31[2019 - 04 - 10].

[13] 张涛,王玥,黄道丽. 信息系统安全治理框架:欧盟的经验与启示——基于网络攻击的视角[J]. 情报杂志,2016,35(8):17 - 24.

(上接第 291 页)

[11] Yang S, Yan D, Wu H, et al. Static control-flow analysis of user-driven callbacks in Android applications[C]//Proceedings of the 37th International Conference on Software Engineering—Volume 1. IEEE, 2015:89 - 99.

[12] Wu D J, Mao C H, Lee H M, et al. DroidMat: Android malware detection through manifest and API calls tracing [C]// Proceedings of the 2012 Seventh Asia Joint Conference on Information Security. IEEE, 2012:62 - 69.

[13] Qu Z, Alam S, Chen Y, et al. DyDroid: measuring dynamic code loading and its security implications in Android applications[C]//2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks(DSN), 2017: 415 - 426.

(上接第 296 页)

[6] Sun D Z, Xu G Q. One-round provably secure yoking-proof for RFID applications[C]//One-Round Provably Secure Yoking-Proof for RFID Applications. IEEE Computer Society, 2017:315 - 322.

[7] Saito J, Imamoto K, Sakurai K. Reassignment scheme of an RFID tag's key for owner transfer[C]//Embedded and Ubiquitous Computing-EUC 2005 Workshops. Springer Berlin Heidelberg, 2005:1303 - 1312.

[8] Elkhiyaoui K, Blass E O, Molva R. ROTIV: RFID ownership transfer with issuer verification[C]//Proceedings of the 7th international conference on RFID Security and Privacy. Springer-Verlag, 2010:163 - 182.

[9] 金永明,孙惠平,关志,等. RFID 标签所有权转移协议研究[J]. 计算机研究与发展,2011,48(8):1400 - 1405.

[10] 沈金伟,凌捷. 一种改进的超轻量级 RFID 所有权转移协议[J]. 计算机科学,2014,41(12):125 - 128.

[11] 李希元,孙超,郑薇. 基于伪随机函数的 RFID 双向认证协议[J]. 计算机工程与应用,2018,54(17):67 - 70.

[12] Xie R, Jian B Y, Liu D W. An improved ownership transfer for RFID protocol[J]. International Journal of Network Security, 2018, 20(1):149 - 156.

[13] 原变青,刘吉强. 可证明安全的 RFID 标签所有权转移协议[J]. 通信学报,2015,36(8):83 - 90.

[14] 陈秀清,曹天杰,翟靖轩. 可证明安全的轻量级 RFID 所有权转移协议[J]. 电子与信息学报,2016,38(8):2091 - 2098.