

我国关键信息基础设施保护的立法思考

黄道丽¹, 方婷²

(1. 公安部第三研究所, 上海 201204;
2. 西安交通大学信息安全法律研究中心, 陕西 西安 710049)

摘要: 我国关键信息基础设施保护立法的必要性尤为突出。现行立法及实践表现为关键信息基础设施保护缺乏国家层面的强力监管, 国家和行业主管部门的认识和保护能力不足, 主管机构的职责不清且缺乏有效的协调配合机制, 资金、技术、人员等基础保障能力薄弱。为加快制定和颁布关键信息基础设施保护立法, 应当明确关键信息基础设施保护的组织机构体系及其工作机制, 构建关键信息基础设施保护的监测通报与预警机制、应急处置与响应恢复机制、安全监管制度、责任追究制度和基础保障制度。

关键词: 关键信息基础设施; 监测; 预警; 应急响应

中图分类号: D035.3

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00033

Legislative reflection on critical information infrastructure protection in China

HUANG Dao-li¹, FANG Ting²

(1. The Third Research Institute of Ministry of Public Security, Shanghai 201204, China;
2. Information Security Law Research Center, Xi'an Jiaotong University, Xi'an 710049, China)

Abstract: The necessity of critical information infrastructure protection legislation is particularly prominent. Current legislations and practice show that critical information infrastructure protection is lack of a strong regulation at the national level, national and industry department lack of knowledge and ability to protect critical information infrastructure and their responsibilities are unclear with no effective coordination mechanisms, financial, technical and personnel support capabilities are also weak. To speed up the formulation and promulgation of critical information infrastructure protection legislation, the organization system and its working mechanism of critical information infrastructure protection should be clearly defined, and early warning and monitoring mechanism, emergency response and recovery mechanisms, security supervision system, accountability system and basic safeguard system should be built.

Key words: critical information infrastructure, monitoring, warning, emergency response

1 引言

2015年6月,第十二届全国人大常委会第十五次会议初次审议了《中华人民共和国网络安全

法(草案)》^[1],其中,在“网络运行安全”一般规定的基础上,设专节对关键信息基础设施的运行安全做出了具体规定并实行重点保护,保护的经营范围包括基础信息网络、重要行业和领域的重要

收稿日期: 2016-02-03; 修回日期: 2016-02-23。通信作者: 方婷, 27562550@qq.com

基金项目: 信息网络安全公安部重点实验室开放课题基金资助项目(No.C13603)

Foundation Item: Information Network Security Key Lab Program of the Ministry of Public Security (No.C13603)

信息系统、军事网络、重要政务网络、用户数量众多的商业网络等。在此基础上,《草案》进一步提出了关键信息基础设施保护的三同步原则,明确了关键信息基础设施保护主管部门的职责和运营者的安全保护义务,建立了关键信息基础设施运营者采购网络产品、服务的安全审查制度,并要求建立关键信息基础设施保护相关部门之间的协作机制等。同时,2015年7月1日颁布实施的《国家安全法》第25条进一步部署了有关关键基础设施和重要领域信息系统及数据安全可控的战略举措。由此可见,我国已经充分认识到关键信息基础设施保护在维护国家安全、经济安全和保障民生中的重要作用,从网络安全基本法层面关注关键信息基础设施保护的迫切需求,基于此,我国应当在《网络安全法(草案)》、《国家安全法》等基本法相关规定的指导下,针对关键信息基础设施保护进行专门立法,构建关键信息基础设施保护的法律制度体系。

2 我国关键信息基础设施保护立法的必要性分析

美国“9·11”恐怖袭击事件发生后,国家关键基础设施在国家安全、社会民生、经济发展和政府事务中的基础性作用不断凸显,并逐步成为保障整个社会持续运转的重要支撑。然而,随着网络与信息技术的普及和高速发展,传统的物理基础设施与信息系统的融合程度不断加深,使关键基础设施部门的信息系统始终面临外部不安全环境所引发的巨大威胁。2014年至2015年初,美国持续发生了一系列大规模网络攻击事件,零售商Target公司、eBay公司、世界最大的家装零售商Home Depot、摩根大通(JPMorgan Chase)、医疗保险公司Anthem、索尼(Sony)电影公司等企业相继遭到破坏性的网络攻击,这一系列事件充分印证了美国作为信息化高度发达的网络强国,在全球化融合的态势下也同样面临严峻的网络安全挑战,尤其是关系其国家安全、社会稳定和持续运转的能源、通信、交通、金融等关键领域,其信息基础设施保障在当前网络安全形势下显得更加迫切和必要。

值得注意的是,当今社会经济全球化、气

候极端化和国际关系综合化的趋势进一步凸显了国家关键信息基础设施保护的复杂性。在此背景下,国际组织和重要国家始终关注对国家关键基础设施以及关键信息基础设施保护战略、立法和组织体系的构建^[2]。其中,欧盟成员国英国、法国、德国、美国、日本、新加坡均针对国家关键基础设施和关键信息基础设施的界定,国家关键行业/部门的确定,国家关键信息基础设施保护的组织机构体系以及国家关键信息基础设施保护的监测通报与预警机制、应急响应与恢复机制,在其国家战略和法律法规中做出了必要的部署和相应的调整,以满足新形势下国家关键信息基础设施保护的迫切需求。目前,我国关键信息基础设施保护立法的必要性尤为突出,主要表现为如下。

1) 基础信息网络和重要信息系统安全隐患严重^[3]。由于各个基础信息网络和重要信息系统的核心设备、技术和高端服务主要依赖国外进口,短期内无法实现自主可控,给我国的信息安全带来了深层次的安全隐患。信息安全建设与信息化建设不同步,建设不规范、不全面。值得注意的是,目前,国内政府部门和企业过分依赖外国品牌的电子产品、信息技术产品,尤其是基础信息网络和重要信息系统的核心软硬件设备(服务器、存储设备、操作系统等),并且,高端服务仍严重依赖于国外,国外产品的采用率高达80%以上,相当一部分信息系统由国外公司提供技术服务。在涉及政府、能源、通信、海关、金融、交通、医疗等国家关键信息基础设施的建设和运营过程中,频频出现美国“八大金刚”的影子,特别是美国思科几乎参与了中国所有大型网络项目的建设,这无疑对我国的网络与信息安全构成了严重威胁,特别是在美国“棱镜门”事件曝光并持续发酵的过程中,我国关键信息基础设施保护立法的必要性进一步凸显。

2) 我国的网络与信息安全保障工作基础较为薄弱^[4]。其中,我国网络与信息建设未能与信息化建设同步进行,具体的实践工作缺乏国家层面整体的制度化指导和有效监管,网络与信息系统安全建设、监管缺乏相应的标准规范,诸多部门安全管理制度和技术防范措施难以有效落

实。因此,由于网络入侵和恶意攻击等行为导致的网络安全事件频发,尤其是针对关键信息基础设施的网络入侵、恶意攻击等缺乏有效的应对处理措施,风险抵御能力较弱,网络基础设施建设中安全系统建设相对滞后。在此背景下,习近平总书记在主持召开中央网络安全和信息化领导小组第一次会议中做出重要指示,其中,在抓紧制定立法规划方面,要求尽快推进关键信息基础设施保护等法律法规的制定和完善。

3 我国关键信息基础设施保护的立法现状及实践存在的突出问题

我国关键信息基础设施保护的相关法律法规主要包括综合及重要领域类规定两大部分,即《国家安全法》、《中华人民共和国突发事件应对法》、《中华人民共和国保守国家秘密法》、《中华人民共和国计算机信息系统安全保护条例》、《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发[2003]27号)、《信息安全等级保护管理办法》(公通字[2007]43号)、《关于加强工业控制系统信息安全管理的通知》(工信部协[2011]451号)、《国家安全监管总局网络运行和信息安全保密管理办法》、《电力行业网络与信息安全监督管理暂行规定》、《中国人民银行信息安全管理规定》、《基础电信企业信息安全责任管理办法(试行)》、《银行、证券跨行业信息系统突发事件应急处置工作指引》、《铁路计算机信息系统安全保护办法》、《通信网络安全防护管理办法》、《互联网网络安全信息通报实施办法》(工信部保[2009]156号)、《中华人民共和国互联网网络安全应急预案》、《民用航空运输机场航空安全保卫规则》、《公共航空运输企业航空安全保卫规则》等。

然而,作为世界上信息化发展最快的国家之一,我国关键信息基础设施保护的实践仍然存在诸多问题,突出体现在以下几个方面。

1) 我国国家关键信息基础设施保护缺乏国家层面的强力监管。我国目前的信息安全监管工作基本与美国前几年的情况类似,仍需不断建立类似由美国强力部门(国土安全部)实施监督管理的机制^[5]。信息安全监管工作技术性强、工作内容复杂,决定了其监管必须由一支成建制的、

体系化的、覆盖全国范围的队伍实行统一管理、统一策略、统一标准、统一运用合理的工作方法,将信息安全监管工作落到实处。

2) 国家和行业主管部门对关键信息基础设施保护的必要性和重要性认识能力不足。从等级保护工作的实施情况可以看出,重要行业/部门对重要信息系统的“重要性”认识不够,进而对国家关键信息基础设施的“关键性”缺乏认识^[6]。虽然通过等级保护工作,各个关键信息基础设施运营单位对自身信息系统的重要性已有一定的认识,但是,很少会从中国、全社会乃至全球的视角看待信息系统的重要性,很难将信息系统安全上升到国家安全、社会稳定的高度进行分析,对信息系统受到破坏后产生的影响没有做出充分评估。大多数情况下,各重要行业/部门仅仅是从一个单位或一个企业的角度进行信息安全保护,缺乏从信息系统到部门、从部门到机构、从机构到行业以及从行业到关键领域之间的相互依赖性分析,导致对信息系统的重要性认识不够,定级过程缺乏风险分析和关键性分析,难以有效制定关键信息基础设施的优先保护计划。

3) 国家有关行业/部门对关键信息基础设施保护的能力不够,并且机构之间的协调配合机制仍需进一步建立和完善^[7]。首先,重要行业/部门对关键信息基础设施的保护能力不够,主要表现为针对网络入侵和恶意攻击的主动发现、查找、防御和应急响应能力仍需不断提高,实践中,我国虽已建立国家关键信息基础设施安全风险监测和预警机制,但是,各个重要行业/部门对国家关键信息基础设施安全风险的监测和预警能力仍然较弱,需要得到进一步加强;其次,省市一级重要行业/部门对关键信息基础设施安全事件的通报能力有待加强,尚未建立包括中央和地方在内的立体的全国性监测通报体系,导致中央和地方之间的重要行业/部门之间难以对网络信息安全事件进行有效的信息共享,降低了各个重要行业/部门发现网络信息安全威胁的能力;最后,我国重要行业/部门对关键基础设施信息安全事件的应急措施不完备,难以对关键基础设施部门突发的信息安全事件进行有效的应急响应与处置。值得注意的是,对涉及跨领域且具有高度相互依赖

性的关键信息基础设施，如电力、电信等，由于缺少社会协调配合机制，主管部门或运营使用单位在进行关键信息基础设施的保护工作时，往往单打独斗，很难通过一个高效的组织方式，协调社会资源参与关键信息基础设施的保护，最终影响保护工作的实施效率。

4) 我国国家关键信息基础设施保护机构的职责不清、分工不明确，导致实践操作中重要信息系统的安全保护要求（关键信息基础设施保护要求）无法得到有效满足。目前，实践中，既存在以公安部为主导的规范化、系统化、制度化、覆盖政府机关和关键信息基础设施的信息安全等级保护工作，也存在每年由工信部主持的仅针对政府部门和个别央企的安全检查工作，还存在如中国人民银行、证监会、银监会、保监会、发改委、科技部、商务部、国家密码管理局、国家保密局、国家质量监督检验检疫总局等非主管部门实施的对关键信息基础设施保护的监督管理，导致多头管理现象明显、重复工作内容很多、职责分工不明，给重要信息系统的运营使用单位带来了极大的困惑，不利于我国关键信息基础设施保护工作的有效实施。

5) 我国国家关键信息基础设施保护的基础保障能力薄弱，在资金保障、技术支持、人员和机构设置以及制度建设等方面无法保障关键信息基础设施保护工作的有效落实。目前，我国国家关键信息基础设施保护规划尚未纳入国民经济和社会发展计划，难以使国家关键信息基础设施保护工作同经济建设和社会发展相协调。同时，国家对关键信息基础设施保护的技术研发和资金支持力度有待进一步加强。

4 我国加强关键信息基础设施立法保护的制度建议

基于前述分析，我国应当从立法层面关注关键信息基础设施保护制度的建立，设立关键信息基础设施保护的强力监管部门，构建关键信息基础设施保护的组织管理体系，建立关键信息基础设施保护监测通报与预警发布中心，建立关键信息基础设施保护的预警机构，建立关键信息基础设施保护的信息共享机制，强调关键信息基础设

施保护的技术支持，关注关键信息基础设施保护的财政保障，注重关键信息基础设施保护的专业人员培养，加强关键信息基础设施保护的国际合作，基于此，我国关键信息基础设施保护立法应当重点包括以下几个方面。

4.1 建立我国关键信息基础设施保护的组织机构及其工作机制

在美国，85%的国家关键基础设施由私营部门拥有和运营管理，而我国的国家关键基础设施多数是由国企或央企运营和管理。由于国情的差异，我国的关键信息基础设施保护制度的构建不能简单照搬外国的经验，但这些关键信息基础设施也严重关系到我国的社会稳定、国计民生和经济发展，对关键信息基础设施的保护同样不能仅仅依赖于单一企业或主管部门的努力，需要协调国家、社会、企业自身等各界的努力来共同实现^[8]。基于此，在充分吸取国外经验和教训的基础上，建立符合我国国情且具有较强可操作性的关键信息基础设施保护组织管理体系是我国关键信息基础设施保护立法亟需解决的重要问题之一。

基于前述分析，本文认为党和政府的支持是我国关键信息基础设施保护的坚实基础，各级政府高度重视；各个部委密切协调合作、配合关键信息基础设施保护的职责机构高效实施保护工作是我国关键信息基础设施保护的坚实保障；各行业主管部门、运营使用单位及其他信息服务部门顾全大局、相互协调、有力执行是我国关键信息基础设施保护的实践基础。因此，建立自上而下、逐级逐层监督管理的组织体系能够保证关键信息基础设施保护工作的有效实施，同时，各级层分别建立协调配合的伙伴关系既能确保对上级指示进行科学有效的执行，也可以为各个部门单位就自身利益提供表述和协调的渠道。简单来说，我国关键信息基础设施保护的组织管理体系应该是：自上而下的监督管理，各级层协调合作的组织关系。

4.2 构建全国立体的关键信息基础设施保护监测通报与预警机制

各个国家在关键信息基础设施保护方面的策略之一即为早期预警，通过建立一套完整的监测、

评价、应急响应体系,以确保在各类网络安全事件发生前能够及时预警并及时响应。为此,各类监测与预警发布中心应运而生,如美国 US-CERT 组织、国土安全部下设的 NCCIC、新加坡国家网络威胁监测中心,都负责全天候监测和分析针对关键信息基础设施的网络威胁信息^[9]。为了更好地预警早期可能发生的事件并能够快速响应,信息共享是早期预警和应急响应机制背后主要的推动力^[10]。公共私营机构共同合作,通过各类方式完成信息共享,从而建立应急响应机制。

基于前述分析,我国建立与完善国家关键信息基础设施安全事件的监测通报与预警机制^[11]应当包括3个方面的内容:1) 我国应当建立与完善省市两级的关键信息基础设施保护监测通报与预警机制,构建全国立体的监测通报与预警体系,提高关键信息基础设施运营单位对信息安全威胁的发现能力、预警能力、防护能力和反制能力;2) 进一步完善关键信息基础设施相关的漏洞通报机制,由国家网络安全主管部门授权相关的信息安全风险监测机构定期发布信息安全漏洞通报;3) 从预警级别、预警启动、不同级别预警的应对机制以及预警解除等方面完善国家关键信息基础设施安全事件的预警机制。

4.3 建立与完善关键信息基础设施保护的应急处置与响应恢复机制

基于前述分析,我国建立与完善国家关键信息基础设施保护的应急处置与响应恢复机制的内容应当包括:1) 建立国家关键信息基础设施安全事件的应急处置基本制度,其中,包括国家关键信息基础设施安全事件的分级处置和标准制定以及应急预案的制定;2) 明确国家关键信息基础设施安全事件的应急处置措施,包括信息安全事件的检测,信息安全事件应急预案的启动以及特大、重大信息安全事件的紧急处置^[12];3) 完善国家关键信息基础设施安全事件的信息发布机制;4) 完善安全事件后国家关键信息基础设施的恢复制度;5) 完善国家关键信息基础设施安全事件应急处置和恢复的总结报告制度。

4.4 建立关键信息基础设施的安全监管制度

基于前述分析,我国构建国家关键信息基础设施的安全监管制度应当包括以下几个方面:

1) 明确公安机关的安全监管职责,涉及指导、协调国家关键信息基础设施安全保护对象的认定、共享依赖性和脆弱性评估、信息安全风险监测通报与预警等^[13];2) 明确各重要行业主管部门的安全监管职责;3) 明确国家关键信息基础设施运营单位的安全监管职责和信息安全服务单位相应的协助义务;4) 明确各级地方政府的安全监管职责。最为重要的是,应当确保关键信息基础设施保护的行业主管与安全主管分离^[14]。

4.5 建立关键信息基础设施保护的责任追究制度

关键信息基础设施保护立法应当建立相应的责任追究制度,以有效贯彻和落实关键信息基础设施保护工作,具体而言,相应的责任主要包括以下方面:国家关键基础设施运营单位怠于行使安全保护制度和措施的法律职责,违反系统检测和评估义务的法律职责;信息安全检测评估机构未经认可或行政许可进行检测评估活动的法律职责,利用职业便利从事侵害他人合法权益活动的法律职责;涉密国家关键基础设施运营单位违反保守国家秘密义务的法律职责;单位或个人破坏、危害基础信息网络与关键信息系统安全的法律职责,违反信息安全事件报告和协查义务的法律职责;国家关键基础设施运营单位的主管部门应急处置行政失职的法律职责;公安机关、国家关键基础设施运营单位的主管部门、各级人民政府以及其他国家机关的工作人员在关键信息基础设施保护过程中失职的法律职责。

4.6 建立关键信息基础设施保护的基础保障制度

1) 从国家层面加强关键信息基础设施保护的人员、资金等支持力度。从国家层面总体上加强关键信息基础设施的基础保障能力,包括人员、资金等支持,具体而言,国家关键信息基础设施保护规划必须纳入国民经济和社会发展规划,国家应当采取有利于信息安全保护的经济、技术政策和措施,使国家关键信息基础设施保护工作同经济建设和社会发展相协调。省级以上地方人民政府将国家关键信息基础设施保护纳入本行政区域的国民经济和社会发展规划。在人员建设方面,国家应当开展信息安全保护教育,尤其是国家关键基础设施运营单

位，应当定期对其工作人员进行国家关键信息基础设施安全保护的知识、技能培训，提高其工作人员对信息安全风险的防范意识和应对能力。在资金保障方面，国家应当加强对关键信息基础设施保护的财政资金支持，省、自治区、直辖市人民政府负责本行政区域内国家关键信息基础设施安全预防、监督工作的日常经费。中央网信办会同国务院有关部门，确定全国国家关键信息基础设施安全事件的监测、预警、应急处置、监督检查等项目，中央财政保障实施经费。中央财政对困难地区实施重大国家关键信息基础设施安全事件处置项目给予补助。

2) 提高关键信息基础设施保护的技术建设能力。国家应当鼓励关键信息基础设施保护领域的科学教育事业的发展，加强国家关键信息基础设施保护（网络安全、侦查打击、管理控制等）技术和相关产品的研究与开发，保障对进行国家关键信息基础设施保护的科学研究、技术开发和教学的科研院所、高等院校和各企事业单位予以相应的经费支持，提高相关从业人员的信息安全科学技术水平。同时，国家应当对在关键信息基础设施保护工作中做出显著成绩和贡献的单位和个人给予表彰和奖励，对于成功开发与关键信息基础设施保护相关研究成果的，对研究人员和机构给予相应表彰和物质奖励。

3) 保障关键信息基础设施的安全可控^[15]。我国应当建立国家关键信息基础设施的产品、服务安全审查制度，同时加快实施关键信息基础设施国产化替代工程。一是加强对信息技术和产品的技术可靠性审查；二是对于国防、政府、商业应用不同类别的信息技术产品审查、检测，实行有区别的管理政策，建立与之相适应的安全审查机制；三是在国家关键信息基础设施采购中，根据产品的来源（国别）、可靠性（国家是否可控和生产单位是否可控）进行供应链审查。此外，在关键信息基础设施领域，确保国家科技重大专项持续支持高端服务器、海量存储、中间件、数据库的研发，支持产业联盟的发展，大力发展集成电路产业，支持我国产业标准的制定，打造完整的、安全可靠的信息系统标准体系，鼓励软件厂商和硬件厂商互相认证、协同发展。

5 结束语

综上所述，我国应当加快制定和颁布关键信息基础设施保护立法，确立关键信息基础设施保护的立法原则，明确关键信息基础设施保护的组织机构体系及其工作机制，构建关键信息基础设施保护的监测通报与预警机制、应急处置与响应恢复机制、安全监管制度、责任追究制度和基础保障制度，以构建关键信息基础设施保护的风险管理框架和相应的技术标准规范体系，落实关键信息基础设施保护的具体工作。

参考文献：

- [1] 第十二届全国人大常委会. 中华人民共和国网络安全法（草案）[EB/OL]. http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm.
The Standing Committee of the 12th NPC. People's republic of China cyber security law (draft)[EB/OL]. http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm.
- [2] BRUMMER E M, SUTER M. CIIP handbook 2008/2009[M]. Beijing: National Defence Industry Press, 2010:296-300.
- [3] 公安部信息安全等级保护评估中心. 信息安全等级保护政策培训教程[M]. 北京: 电子工业出版社, 2010:45-52.
MPS Information Classified Security Protection Evaluation Center. Information classified security protection policy training course[M]. Beijing: Publishing House of Electronics Industry, 2010:45-52.
- [4] 马民虎. 网络安全法律问题及对策研究[M]. 西安: 陕西科学技术出版社, 2007:171.
MA M H. Cyber security legal problems and countermeasures research[M]. Xi'an: Shanxi Science and Technology Press, 2007:171.
- [5] 美国通信行业协会. 保障网络安全: 保障关键基础设施和全球供应链的建议[R/OL]. http://www.usito.org/sites/default/files/tia_cybersecurity_white_paper-critical_infrastructure_global_supply_chain-chinese-201306.pdf.
The American Association of Communication Industry. Securing the network: cyber security recommendations for critical infrastructure and the global supply chain[R/OL]. http://www.usito.org/sites/default/files/tia_cybersecurity_white_paper-critical_infrastructure_global_supply_chain-chinese-201306.pdf.
- [6] GEORGE R. Critical infrastructure protection[J]. Journal of Healthcare Protection Management Publication of the International Association for Hospital Security, 2012, 28(2):11-15.
- [7] RICE M, BUTTS J, MILLER R, et al. An analysis of the legality of government-mandated computer inoculations[J]. International Journal of Critical Infrastructure Protection, 2010, 3(1):5-15.
- [8] CLAVADETSCGER C J. Building national resilience capabilities[J]. International Journal of Critical Infrastructure Protection, 2010, 3(1):27-28.

- [9] COHEN F. What makes critical infrastructures critical?[J]. International Journal of Critical Infrastructure Protection, 2010, 3(3): 53-54.
- [10] MAHONEY W, GANDHI R A. An integrated framework for control system simulation and regulatory compliance monitoring[J]. International Journal of Critical Infrastructure Protection, 2011, 4(1):41-53.
- [11] 王玥, 方婷, 马民虎. 美国关键基础设施信息安全监测预警机制演进与启示[J]. 情报杂志, 2016 (1): 17-23.
WANG Y, FANG T, MA M H. Analysis and enlightenment of the evolution of the US critical infrastructure information security monitoring and warning mechanism[J]. Journal of Intelligence, 2016(1):17-23.
- [12] 张莉. 美国保护关键基础设施安全政策分析[J]. 信息安全与技术, 2013(7): 3-6.
ZHANG L. The analysis of US policy on protecting critical infrastructure security[J]. Information Security and Technology, 2013(7): 3-6.
- [13] 马民虎. 信息安全法研究[M]. 西安: 陕西人民出版社, 2004: 289.
MA M H. Information security law research[M]. Xi'an: Shanxi People's Publishing House, 2004: 289.
- [14] 曲洁, 朱建平. 等级保护与关键基础设施防护的融合研究[J]. 信息网络安全, 2011 (12): 84-88.
QU J, ZHU J P. The research of combination of classified protection and critical infrastructure protection[J]. Information Network Security, 2011(12):84-88.
- [15] 孙丕恕. 加强关键信息基础设施安全保障能力[EB/OL]. <http://npc.people.com.cn/n/2014/0307/c376899-24567166.html>.
SUN P S. Strengthen the security assurance capabilities of critical information infrastructure[EB/OL]. <http://npc.people.com.cn/n/2014/0307/c376899-24567166.html>.

作者简介:



黄道丽(1980-), 女, 湖北公安人, 公安部第三研究所信息网络安全公安部重点实验室研究员, 主要研究方向为电子数据鉴定、计算机取证、网络与信息安全法学。



方婷(1987-), 女, 江苏南京人, 西安交通大学博士生, 主要研究方向为信息安全法。