主题研讨

我国网络关键基础设施立法的基本思路和制度建构

刘金瑞

内容提要:关键基础设施保护已成为各国网络安全治理和立法的核心议题。域外立法以美国为代表,重点是私营关键基础设施保护和网络安全信息共享,现行制度框架包括五个方面:建立政府和行业的协作机制,制订国家级保护计划,设立信息共享和分析中心,认定关键设施、评估漏洞风险和确定优先防护措施,制订网络安全框架。借鉴域外法治经验,针对我国关键基础设施立法提出如下建议:一是从国家安全高度把握关键基础设施的界定和立法的体系化;二是坚持国内外经验相结合,将网络安全分为"系统安全"和"内容安全",处理好关键基础设施保护和信息安全等级保护的关系;三是区分一般信息系统和关键基础设施、区分公共部门和私营部门来设计监管框架;四是坚持安全与发展并重,构建政府和企业的协作机制,完善网络安全信息共享和企业责任豁免;五是规定法律的域外效力和针对网络攻击的反制措施,为国际规则制定留有空间。

关键词:关键基础设施保护　网络安全立法　网络安全信息共享

刘金瑞,中国法学会法律信息部助理研究员。

一　关键基础设施保护是网络安全立法的核心

当前,网络信息浪潮席卷全球,已经革命性地改变了人类的社会生活方式。随之出现的网络安全问题给人类社会带来了新的巨大挑战,网络安全的治理和立法已经成为一个全球性的议题。

(一)网络安全的核心是保护关键基础设施

随着信息通信技术的迅速进展,金融系统、交通运输、电力网线、电信服务、供水管线以及政府服务等基础设施的运营日益依靠网络信息系统,人类的日常行为日益转变为网络空间的信息数据流。然而,互相连接、互相依赖的网络信息系统极其容易因为其所附着的基础设施受损、被拒绝服务攻击等而陷入瘫痪,网络信息系统内的信息数据也极其容易被拦截、窃取和破坏,从而引发了网络安全的问题。

对于网络空间的安全问题,美国立法界定为“信息安全(information security)”,是指“保护信息和信息系统不受未经授权的访问、使用、披露、破坏、修改或者销毁”,以确保信息的完整性、保密性和可用性。[1] 欧盟立法将其界定为“网络和信息安全(network and information security,NIS)”,是指“网络或者信息系统在一定的可信度下抵御突发事件、非法或者恶意行为的能力,这些行为会危害该系统所存储或传输的数据的可用性、真实性、完整性以及保密性,危害通过该网络或者系统提供的或者获得的相关服务。”[2]网络安全就是要确保网络信息系统[3]及其所存储和传输的数据的安全。

从世界范围的网络安全政策和立法来看,[4]核心内容就是要保护事关国家安全、公共安全的关键基础设施(Critical Infrastructure),保护这些基础设施所依赖的网络信息系统及其所存储和传输的数据。关键基础设施面临的安全风险不仅包括自然灾害等物理威胁,更包括各国网络安全立法所强调的针对信息系统的网络威胁,表现为黑客入侵、电子间谍、网络盗窃甚至令人担忧的网络战争、网络恐怖主义等。[5]

这并非杞人忧天:2010 年 9 月摧毁伊朗核电站离心机的 Stuxnet 病毒,据媒体披露是由美国与以色列共同研发,[6]该病毒后感染世界各地,我国也深受其害;2013 年 6 月,美国中央情报局前雇员斯诺登披露,美国国家安全局曾持续攻击清华大学的教育网主干网,为获取手机短信信息而广泛入侵中国的主要电信运营商;[7]近年来,针对我国关键基础设施和特定目标的高级持续性威胁(APT)攻击频现,例如 2015 年曝光的境外“海莲花”黑客组织多年以来针对我国海事机构实施 APT 攻击以及长期针对我国政府机构实施攻击的 APT-TOCS 事件;2015 年,国家信息安全漏洞共享平台发现境外有千余个 IP 地址渗透扫描我国大量使用的某款工业控制系统,有数百个 IP 地址访问过我国互联网上暴露的

---

〔1〕 Federal Information Security Management Act, 44 USC § 3542(b)(1). 在美国版权法的某些条款中,将“信息安全”界定成“为了确定和解决政府电脑、电脑系统或者电脑网络漏洞而采取的行为”,Copyright, 17 U. S. C. 1201 (e), 1202(d).

〔2〕 *Regulation No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency*, art. 4(c), OJ L 77, 13. 3. 2004, p. 5; *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on Network and Information Security: Proposal for A European Policy Approach*, COM (2001) 298 final, 6. 6. 2001, p. 9.

〔3〕 “信息系统(information system)”是指计算机和电子通信网络,以及它们为了自身的运行、应用、保护及维持的目的所存储、处理、存取或者传输的电子数据,见 *Regulation No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency*, art. 4(b), OJ L 77, 13. 3. 2004, p. 5.

〔4〕 参见下文对美国网络安全政策和立法的梳理介绍;European Network and Information Security Agency, *National Cyber Security Strategies: Setting the Course for National Efforts*, May 2012, http://www. enisa. europa. eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper/at _ download/fullReport, last visited on Jul. 29, 2016.

〔5〕 这些指称网络攻击行为的称谓并不是截然区分的,某个行为可能同时属于多个称谓。

〔6〕 David Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, http://www. nytimes. com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran. html? pagewanted = all&_r = 0, last visited on Jul. 3, 2016.

〔7〕 *Snowden Reveals more US Cyberspying details*, in *South China Morning Post*, Jun. 23, 2013, http://www. scmp. com/news/hong-kong/article/1266777/exclusive-snowden-safe-hong-kong-more-us-cyberspying-details-revealed, last visited on Jul. 29, 2016.

工业控制设备。[8] 鉴于关键基础设施关系到国家命脉和社会运行,上述威胁对国家安全、公共安全和社会稳定造成了极大的挑战,关键基础设施保护已成为各国网络安全治理和立法的核心内容。

(二)关键基础设施概念的界定

美国最早开始关注关键基础设施保护,并逐步探索法律保护框架。1996 年 7 月,克林顿政府颁布《第 13010 号行政命令》(以下简称 E. O. 13010),首次提出关键基础设施不仅面临物理威胁,也面临该设施信息或通信部分遭受攻击的网络威胁。[9] 1998 年 5 月,克林顿政府颁布《第 63 号总统决策指令》(以下简称 PDD-63),将关键基础设施界定为"物理的或基于网络的、维持经济及政府最低程度运行所必需的系统"。[10]

2001 年 10 月,小布什政府颁布《美国爱国者法案》(USA PATRIOT Act),[11] 将"关键基础设施"定义修改为"对于美国来说极其重要的物理的或虚拟的系统和资产,一旦它们能力丧失或遭到破坏,就会削弱国家安全、国家经济安全或者国家公众健康与安全"。该定义为之后的美国立法所沿用。[12] 2013 年,奥巴马政府的《第 21 号总统政策指令》[13](以下简称 PPD-21)认为关键基础设施涉及通信、信息技术、金融服务、政府设施、交通系统、商业设施、关键制造、能源等 16 个领域。

2016 年 8 月,欧盟《关于欧盟共同的高水平网络与信息系统安全措施的指令》(以下简称 NIS 指令)正式生效,欧盟各成员国要在 2018 年 5 月 9 日之前将其转化为国内法。指令并没有采用"关键基础设施"的概念,而是使用了"基本服务运营者"的表述。所谓"基本服务运营者",是指"提供维续关键社会活动及/或经济活动基本服务的主体,该服务的提供依赖于网络和信息系统,网络安全事件会对该服务的提供造成重大的破坏性影响",涉及能源(电力、石油及天然气)、运输(航空、铁路、水运及陆运)、银行、金融市场基础设施、医疗卫生、饮用水供应分配以及数字基础设施(互联网交换点、域名系统服务提供者及顶级域名注册)领域。[14]

作为欧盟成员国的德国于 2015 年 8 月 14 日通过了《加强联邦信息技术安全法》修正案,增加了"关键基础设施"的定义,是指"对于德国共同体的运作具有重大意义的设施、设备或者其组成,一旦停止运作或者遭受损害将造成严重的供应紧张或者对公共安全产

〔8〕 国家互联网应急中心主编:《2015 年中国互联网网络安全报告》,人民邮电出版社 2016 年版,第 17 页。

〔9〕 Executive Order 13010: Critical Infrastructure Protection, Federal Register, Vol. 61, No. 138, July 15, 1996, pp. 37347 - 37350.

〔10〕 Presidential Decision Directive 63: Critical Infrastructure Protection, May 22, 1998, http://www.fas.org/irp/offdocs/pdd/pdd-63.htm, last visited on Jul. 29, 2016.

〔11〕 该法案的全称为"Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001",译为"2001 年使用适当的手段来阻止或避免恐怖主义以团结并强化美国的法案",取英文原名的首字缩写成为"USA PATRIOT Act",译为"美国爱国者法案"。

〔12〕 USA PATRIOT Act, Title X, Sec. 1016. Critical Infrastructures Protection Act of 2001, 42 USC § 5195c.

〔13〕 Presidential Policy Directive 21: Critical Infrastructure Security and Resilience, February 19, 2013, http://www.fas.org/irp/offdocs/ppd/ppd-21.pdf, last visited on Jul. 29, 2016.

〔14〕 *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*, OJ L 194, 19.7.2016, p. 13 - 14, 27 - 29.

生严重威胁”,涉及能源、电信、信息技术、交通运输、卫生、食品以及金融保险领域;具体范围由联邦政府以法规命令予以规定,但明确排除了这些领域中的小企业。[15]

可以发现,无论是美国还是欧盟,都将关键基础设施保护上升到维护国家安全和公共安全的高度,在界定“关键基础设施”及其范围时强调国家安全和公共安全,所谓的“关键”就是指事关国家安全和公共安全,这既突出了保护的重点,也避免了将过多企业纳入监管而徒增企业负担。

近年来,面对严峻的网络安全形势,我国高度重视关键基础设施保护。2015 年 7 月 1 日通过的《国家安全法》第 25 条明确规定:“实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控”。全国人大常委会审议的《网络安全法(草案二审稿)》(以下简称“二审稿”)的第 3 章“网络运行安全”对此有专门规定,并明确“关键信息基础设施的具体范围和安全保护办法由国务院制定。”2016 年 3 月,《关键信息基础设施安全保护条例》纳入国务院 2016 年立法工作计划的研究项目。

2016 年 4 月 19 日,习近平总书记《在网络安全和信息化工作座谈会上的讲话》更是明确指出:“金融、能源、电力、通信、交通等领域的关键信息基础设施是经济社会运行的神经中枢,是网络安全的重中之重,也是可能遭到重点攻击的目标。……不出问题则已,一出就可能导致交通中断、金融紊乱、电力瘫痪等问题,具有很大的破坏性和杀伤力。”习总书记的讲话已经将关键基础设施保护提升到维护国家安全和公共安全的高度,深入研究和系统构建关键基础设施保护的法律制度尤为迫切。

本文就是在这一背景下,针对我国面临的严峻挑战和立法难题,在观察分析域外法治进展的基础上,结合《网络安全法(草案二审稿)》的修改完善,提出我国关键基础设施立法的基本思路和制度建构,以期能够对我国关键基础设施保护和网络安全立法提供有益参考。

二 域外关键基础设施保护立法的制度架构
——以美国为例

美国作为全球网络信息技术最发达的国家,很早就认识到了堪称“电子阿基里斯腱”的网络安全挑战,[16]从 20 世纪 90 年代后期就逐步开始研究应对策略和探索法制框架。美国网络安全立法的核心就是关键基础设施保护,它的战略政策和法令立法逐步推进,基本经历了从政策到立法、从国内到国际的演进过程,从克林顿政府行政命令的被动应对到小布什政府《网络空间安全国家战略》的主动防御、再到奥巴马政府《网络空间国际战略》

〔15〕 Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes, BGBl. I S. 2821, §2(10), §8c(1), http://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html, last visited on Jul. 29, 2016.

〔16〕 James A. Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, Center for Strategic and International Studies, http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf, last visited on Jul. 29, 2016.

的国际威慑,美国网络安全风险应对策略逐渐走向全面和成熟。[17] 在战略全面成熟之后,美国奥巴马政府开始推动网络安全的综合性立法。

(一)美国关键基础设施保护立法的基本思路

对于网络安全和关键基础设施保护,美国有超过 50 部联邦法律直接或间接有关,但至今没有一部统一的框架性立法。奥巴马政府上台以来,开始推动网络安全的综合性立法,其中最为重要的两个议题是"保护私营关键基础设施"与"促进网络安全信息共享"。[18] 对于前者,美国的立法设想集中体现为《2012 年网络安全法案》[19](以下简称 S. 2105)的相关规定,但至今未获通过。只侧重"保护私营关键基础设施"的原因是,美国对政府关键基础设施部署了"爱因斯坦"计划[20]以应对威胁,但对于大部分的私营关键基础设施来说,美国政府不可能强行将其纳入"爱因斯坦"检测防御系统,只能寻求其他监管方案。对于后者,美国的立法设想集中体现为 2015 年 12 月签署生效的《网络安全信息共享法》[21](以下简称 CISA)。这两个议题是关键基础设施保护立法的两大重点,以下结合 S. 2105 和 CISA 的相关规定对美国的立法思路作一简要介绍。

1. 保护私营关键基础设施的立法思路

S. 2105 是唯一进入参议院全体辩论(S. 3414)的法案,是目前美国国会关于网络安全综合性立法最重要的法案。主要立法思路是:授权国土安全部划定关键基础设施的范围,并赋予这些设施以强制性的监管方案和安全标准。其主要内容包括:

(1)明确了"关键基础设施"的定义。所谓关键基础设施,是指一旦被未经授权地损害或者访问,便很可能会导致生命维持服务中断的系统或资产,这种服务中断足以导致大规模伤亡事件、全国性长时间停工、灾难性经济损害或者国家安全严重恶化。"灾难性经济损害"是指美国金融市场、交通系统的崩溃或根本性破坏,或者对美国经济造成其他长期系统性的损害。[22] 但关键基础设施不包括"商业性信息技术产品"。[23]

(2)对关键基础设施的特定系统和资产设立监管方案。国土安全部负责确认关键基础设施的网络安全威胁,有权认定纳入关键基础设施监管范围的资产或者系统,并且确定其为抵御已认定的网络安全威胁而应该具备的性能标准。纳入关键基础设施监管范围的资产或者系统必须遵守该法设立的监管方案。关键基础设施的所有者可以将其系统或资产自行认定或者请求国土安全部认定为关键基础设施。[24]

---

〔17〕 美国网络安全政策战略的演进,参见刘金瑞:《美国网络安全的政策战略演进及当前立法重点》,《北航法律评论》2013 年第 1 辑(总第 4 辑),第 209 - 218 页。

〔18〕 对于美国网络安全综合性立法的相关法案及内容介绍,参见刘金瑞:《美国网络安全立法近期进展及对我国的启示》,《暨南学报(哲学社会科学版)》2014 年第 2 期,第 77 - 78 页。

〔19〕 S. 2105, Cybersecurity Act of 2012, February 14, 2012, http://www.gpo.gov/fdsys/pkg/BILLS-112s2105pcs/pdf/BILLS-112s2105pcs.pdf, last visited on Jul. 29, 2016.

〔20〕 该计划旨在联邦政府网络部署入侵检测系统和入侵防御系统,美国国内对该计划的争议很大,主要问题在于这些系统可能会违反《美国宪法第四修正案》以及侵害个人隐私和公民自由。

〔21〕 Cybersecurity Information Sharing Act of 2015, https://www.congress.gov/bill/114th-congress/senate-bill/754, last visited on Jul. 29, 2016.

〔22〕 S. 2105, § 103.

〔23〕 该法案将其界定为"通过电子方式组织或传递信息的商品",S. 2105, § 2(1)。

〔24〕 S. 2105, § 102 - 104.

(3)规定不遵守监管标准所承担的法律责任。明确国土安全部有权规定征收民事罚款,以处罚关键基础设施所有者或运营者不遵守监管标准的行为。要求关键基础设施所有者或运营者每隔三年自我证明或者通过第三方评估其遵守监管标准的情况,但是国土安全部有权在合理怀疑存在违反监管标准的情况下进行审核和检查。只要正在经受威胁的关键基础设施的所有者或运营者,已经遵守了该法规定的监管标准,已经顺利通过了评估以及在事件发生时仍在实质性地遵守标准,就可以豁免民事惩罚性赔偿。[25]

(4)规定国土安全部可以从关键基础设施收集有关信息。为了风险评估以及评价性能标准遵从情况,国土安全部部长有权决定收集关键基础设施的相关信息,这些信息属于美国《关键基础设施信息法》所界定的"关键基础设施信息"(CII),根据美国《信息自由法》的规定,这些信息不适用关于政府信息公开的要求。[26]

在美国,S.2105 及类似私营关键基础设施保护立法引发的主要争议包括:(1)行政决定可能引发的行政诉讼问题。将私主体纳入关键基础设施范围并要求其承担强制性义务,如果这些私主体不服行政决定,可能会对国土安全部提起行政诉讼。(2)纳入强制监管方案而引发的责任承担问题。关键基础设施运营者,不仅因为不遵守相关强制安全标准而可能承担行政责任或者刑事责任,而且可能因为不遵守监管标准这种注意义务而构成法律上的当然过失(Negligence per se),[27]需要承担民事损害赔偿责任。

2.促进网络安全信息共享的立法设计

2015 年 12 月 18 日,CISA 在争议中签署生效,以激励联邦政府和企业为了国家安全而共享网络威胁信息。主要立法思路是通过交换和共享安全信息,来预防和充分应对网络安全事件,以减少损害发生。其主要内容包括:

(1)联邦政府共享网络威胁信息。授权联邦政府共享非机密的"网络威胁指标"和"防御措施"——关于表明网络是如何被攻击以及这些攻击是如何被成功检测、预防或者减轻的,二者统称为"网络威胁信息";授权不仅可以在政府机构间分享此种非机密的信息,也可以与企业和公众分享;机密的网络威胁信息在政府机构之外的共享,仅限于具有适当安全资质的主体;要求联邦政府定期发布"网络安全最佳实践",以帮助小型企业应对其面临的网络安全挑战。[28]

(2)授权企业为了网络安全目的可以监控其自身的信息系统以及所有存储、处理和传输在该系统内的信息,完全豁免企业因为此种监控而可能承担的法律责任。[29]

(3)企业共享网络威胁信息。授权企业与七大特定政府机构分享网络威胁信息,这些机构包括国防部(包括国家安全局)、国家情报总监办公室、国土安全部;企业同样豁免因共享而可能承担的法律责任;规定企业与联邦政府共享网络威胁信息,不影响其他保护性法律的适用,比如保护商业秘密的规定仍然适用。[30]

---

〔25〕 S.2105, §105.

〔26〕 The Freedom of Information Act, 5 U.S.C. §522(d)(3).

〔27〕 程啸、张发靖:《现代侵权行为法中过错责任原则的发展》,《当代法学》2006 年第 1 期,第 92 页。

〔28〕 CISA, Sec.103.

〔29〕 CISA, Sec.104.

〔30〕 CISA, Sec.105.

(4)隐私保护。要求联邦政府保存、使用或者传播网络威胁信息时,必须保护这些网络威胁信息里任何可识别的个人信息不被未经授权地使用或者披露;要求企业标明其所共享的网络威胁信息中的个人信息,删除和网络安全威胁没有直接关系的个人信息;规定发布相关指南,协助企业识别可能包含个人信息的网络威胁信息。[31]

(5)后续行动。根据 CISA,制定了四个相关程序和文件。除了 2016 年 2 月制定的联邦政府向非联邦机构共享网络威胁信息(包括"网络威胁指标"和"防御措施")的程序规定之外,还包括 2016 年 6 月 15 日发布的"非联邦机构向联邦机构共享网络威胁信息指南"、"联邦政府接收网络威胁信息程序"和"隐私和公民自由保护指南"。[32]

在美国,CISA 和类似网络安全信息共享立法引发的争议主要包括:(1)企业采取技术措施监控自身网络系统设施或者共享网络威胁信息的行为,可能违反《电子通信隐私法》(ECPA)等隐私权保护的法律规定,[33]CISA 对此虽然规定了企业责任豁免,但争议仍然存在。(2)豁免企业共享信息的法律责任,主要有两方面的争议:一方面私主体对这种豁免仍存在不信任,联邦机构可能以此作为不利于当事人的证据用于行政执法等;另一方面,责任豁免如涉及舍弃第三方私主体的合法权益,其正当性会受到质疑。(3)共享信息可能会侵害企业的商业利益。类似商业秘密等商业信息,可能发生泄露而被竞争对手获取。因此,企业一般不愿与政府共享涉及商业利益的信息,此类立法的实际成效可能有限。

(二)美国关键基础设施保护制度的实施框架

美国关键基础设施保护立法至今没有通过一部综合性立法,其通过一系列政策文件和行政法令构建了关键基础设施保护的制度框架。本文将这一制度框架梳理为以下五个方面,以清晰地展示出美国制度运行的实际情况,为我国相关立法和制度设计提供有益借鉴。

1. 建立政府和行业的协作机制

为实现政府和行业在保护关键基础设施方面的合作,1998 年 PDD-63 开始指定联邦的不同部门作为相关行业基础设施保护的领导部门,布什政府和奥巴马政府通过行政命令多次调整行业分类和所对应的领导部门。2013 年 PPD-21 法令确定的有 16 种行业分类和对应的领导部门,例如财政部负责金融服务领域,国土安全部负责电信、信息技术、化学、商业设施等领域。

PDD-63 要求每个行业的领导部门选任代表该部门的"行业联络官"和代表行业设施所有者/运营者的"行业协调员"。1999 年 12 月,一些行业自发确立了"关键基础设施安全伙伴关系",以分享安全信息和策略,维护跨行业间的依存关系。国土安全部不是该合作伙伴关系的一部分,但是起到了联络作用,为其举行会议提供行政支持。这一合作伙伴关系联络协调其成员为国家相关战略和国家保护计划的制订提供支持。

---

〔31〕 CISA, Sec. 105.

〔32〕 *DHS, DOJ Release 4 Final Guidance Documents on Cyber Threat Data Sharing*, http://www.executivegov.com/2016/06/dhs-doj-release-4-final-guidance-documents-on-cyber-threat-data-sharing/, last visited on Jul. 29, 2016.

〔33〕 Aaron J. Burstein, Amending the ECPA to Enable a Culture of Cybersecurity Research, *Harvard Journal of Law & Technology*, 2008, p. 167.

之后,小布什政府提出了一个新的"关键基础设施保护伙伴关系模式",将 PDD-63 要求的行业联络官和行业协调员发展成"政府协作委员会"和"行业协作委员会",扩大了政府和所有者/运营者的代表范围。"政府协作委员会"包括州、地方和部落的政府机构。"行业协作委员会"建立自身架构和领导体制,独立于联邦政府运行。在这种模式下,之前跨行业的"伙伴关系"发展为"私营部门跨行业委员会"。行业协作委员会为国家关键基础设施保护计划(NIPP)和特定行业保护计划(SSP)制订提供支持。[34]

2006 年 3 月,国土安全部根据《国土安全法》[35]的授权建立了不适用《联邦咨询委员会法》的"关键基础设施伙伴关系咨询委员会"(CIPAC),这个委员会的会议和文件可以不向公众公开,但国土安全部会公开会议的时间和合适的议程。国土安全部是这个委员会的秘书单位。它的成员包括行业协作委员会的行业成员,也包括州、地方和部落的政府机构。

2. 制订国家关键基础设施保护计划

从 1996 年克林顿政府第 13010 号命令开始,就要求拟订国家关键基础设施保护的相关计划和对策。1998 年,克林顿政府的 PDD-63 要求制订"国家基础设施保障计划";2000 年,克林顿政府卸任之前,提出了《信息系统保护国家计划》(NPISP),但并没有实施。[36]"9·11"事件之后,2001 年小布什政府的第 13231 号行政命令、《国土安全法》、2003 年《网络安全国家战略》都有类似的要求,尤其是 2003 年小布什政府的《第 7 号国土安全总统指令》(以下简称 HSPD-7)明确要求制定综合性计划,保护 14 类国家关键基础设施和重点资源(CIKR),重点资源指"维持经济与政府最低程度运行必需的公有或私营的资源",HSPD-7 将重点资源细化为水坝、政府及商业设施。[37]

国土安全部未能在 2004 年底前按指令要求如期发布计划,直到 2006 年 6 月,小布什政府第一次正式发布国家关键基础设施保护计划(以下简称 NIPP)。因为 HSPD-7 设定了保护 CIKR 的政策目标,该计划不再仅限于防范恐怖主义,还包括预防天然灾害,强调增强国家事前准备、突发事件应对以及灾后及时恢复等;联邦相关部门分别负责 18 种关键基础设施和重点资源(CIKR),并负责制订"特定行业保护计划"(SSP)。NIPP 于 2009 年第一次更新,部分特定行业保护计划也随之更新,2010 年决定将每四年更新一次。

2013 年 2 月,奥巴马政府颁行《第 13636 号行政命令》[38](以下简称 E. O. 13636)以及保障该命令顺利执行的《第 21 号总统政策指令》(PPD-21)。随后,根据 PPD-21 的要求,NIPP 第二次更新,新计划保留了之前基本的伙伴关系模式和风险管理框架,涉及 16

---

〔34〕 U. S. Congress General Accountability Office, *Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics*, GAO-07 - 39, October 2006.

〔35〕 Homeland Security Act of 2002, Public Law 107 - 296—Nov. 25, 2002.

〔36〕 The White House, *Defending America's Cyberspace: National Plan for Information Systems Protection (Version 1.0)*, January 2000, http://www.fas.org/irp/offdocs/pdd/CIP-plan.pdf, last visited on Jul. 29, 2016.

〔37〕 Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection, 39 Weekly Compilation of Presidential Documents, p. 1816, December 17, 2003.

〔38〕 Executive Order 13636: Improving Critical Infrastructure Cybersecurity, Federal Register Vol. 78, No. 33, February 19, 2013, pp. 11737 - 11744.

种行业,但信息技术业和电信业等特定行业保护计划并没有更新。

3. 设立信息共享和分析中心

1998 年,PDD-63 规定联邦调查局内部的"国家关键基础设施保护中心"(NIPC)负责维持政府和私营部门之间相关信息的流通和共享;与之相对,规定私营行业建立信息共享和分析中心(以下简称 ISAC),负责收集、分析和共享其成员间的安全事件信息和应对信息,促成政府和私营行业之间的信息交换。这一设想最后发展成每个行业都有一个信息共享和分析中心。ISAC 和前述行业协作委员会的不同之处在于,ISAC 是 24 小时、365 天全天候运行的,设施运营者的安全事件报告和来自政府的威胁信息,都通过该中心被通报、分析和共享。

虽然 PDD-63 将 ISAC 设想成交换关键基础设施信息最主要的渠道,但国土安全部还是发展出了一系列其他的信息交换系统和机制。除了行业协作委员会,美国计算机应急中心(US-CERT)[39]接受安全事件报告,公布最新的计算机漏洞威胁信息以及特定安全事件应对信息,也负责国家网络警报系统,任何组织或者个人都可以订阅这一系统的通报信息。国土安全部还开发了国土安全信息网络(HSIN),最初是作为联邦、州和地方基层政府执法机构交流和分析威胁信息的主要通信网络。现在 HSIN 提供 50 个州、5 个领地、50 个城市与国土安全部国家行动中心的实时连接。HSIN 现正扩展到包含每个关键基础设施行业(称为 HSIN-CI),作为关键基础设施保护伙伴关系模式的一部分。

"9·11"事件之后,国土安全部建立了"关键基础设施保护行政通知服务处"(ENS),该部门直接联系国土安全部和主要产业公司的首席执行官。ENS 负责向合作伙伴警示关键技术设施安全事件、发布警告产品和组织电话会议。国土安全部还负责运营不依靠公共交换电话网和互联网的"关键基础设施警告网络"(CWIN),为国土安全部与其他政府机构、私营行业和国际机构提供安全通信。

此外,2002 年《国土安全法》要求建立"信息共享和分析组织"(以下简称 ISAO),其是指"公共部门或私营行业组织建立或雇佣的,以收集、分析、交流或者披露关键基础设施信息为目的的正式或非正式组织",以有助于检测、减轻或者恢复关键基础设施所遭受的损害。[40] 根据 PDD-63 建立的 ISAC 是行业导向的,而《国土安全法》界定的 ISAO 没有此种要求。2015 年 2 月,奥巴马政府的《第 13691 号行政命令》[41](E. O. 13691)要求国土安全部长支持这些组织的发展,以促进网络安全信息分享。

4. 授权国土安全部认定关键设施、评估漏洞风险和确定优先防护措施

2002 年《国土安全法》授权国土安全部负责以下任务:(1)从各种各样的渠道获取、接收、分析和整合信息,以识别和评估恐怖主义威胁的性质和范围;(2)开展美国重点资源和关键基础设施漏洞的综合性评估,以明确特定攻击类型引发的风险;(3)整合相关信息,分析漏洞评估,以确定优先的保护和支撑措施。而且,根据小布什政府的《关键基础

〔39〕 该中心承担了国家关键基础设施保护中心(NIPC)的大部分职能。

〔40〕 Critical Infrastructure Information Act of 2002, 6 U. S. C. 131 (5).

〔41〕 E. O. 13691: Promoting Private Sector Cybersecurity Information Sharing, Federal Register, Vol. 80, No. 34, February 20, 2015, pp. 9347 - 9353.

设施和重要资产的物理保护国家战略》,[42]国土安全部还负责:“与其他主要利益相关者合作,发展一套以国家层面的关键性标准来识别设施、系统和功能的统一方法,以有助于确立优先保护者;建立一个综合性数据库,编录这些关键设施、系统和功能;维持一种针对关键行业漏洞和应备措施而不断更新的综合性评估”。奥巴马政府的 PPD-21 指令重申了这些职责。

国土安全部通过不同的机制,包括依靠通过州国土安全官员和行业领导机构官员以及“国家基础设施模拟与分析中心”(NISAC)[43]和“关键基础设施分析办公室”的分析等方式,来认定符合关键基础设施定义的关键基础设施资产。国土安全部将关键基础设施资产分为国内和国外两类,分别纳入“国家关键基础设施优先保护计划”(National Critical Infrastructure Prioritization Program)和“关键海外依存行动计划”(Critical Foreign Dependencies Initiative),两种计划对应了两类秘密的关键基础设施列表数据库。国土安全部通知这些资产的所有者或运营者,帮助他们进行更为具体的漏洞/恢复能力评估,并对如何减轻风险提供建议。此外,国土安全部还负责地区性恢复能力评估计划(RRAP),将漏洞评估扩展到在特定地理区域的关键基础设施和重要资源集群。评估结果将与相关参与人分享,包括设施的所有者或运营者、州和地方政府。是否参与这些评估是自愿的,是否采纳减少风险的建议也是自愿的。即使这些建议被采纳,国土安全部也不会去追踪这些建议的实施情况。

5. 制订网络安全框架

在推动国会立法受阻之后,奥巴马政府于 2013 年颁行 E. O. 13636 和 PPD-21,要求国家标准和技术研究院(NIST)负责制定网络安全技术标准,制定保护关键基础设施的“网络安全框架”。具体要求该框架保持技术中立,反映跨领域的自发共识标准和行业最佳实践,必要时审查并更新,特定领域领导部门配合审查并制订特定领域指南,该框架的安全标准将纳入政府采购计划和合同管理。[44] 这一框架是国土安全部负责建立的“自愿关键基础设施网络安全计划”的基础。此外,E. O. 13636 要求国土安全部参考特定行业部门的认知,通过协商机制来认定关键基础设施列表并且每年予以更新,明确那些一旦发生网络安全事件,就可能造成地区性或者全国性的公共健康或安全、经济安全和国家安全方面灾难性后果的设施,但明确排除了商业信息技术产品或消费信息技术服务;秘密通知列表设施的所有者和运营者,鼓励他们采用基于“网络安全框架”的“关键基础设施网络安全计划”,所有者和运营者对纳入秘密设施列表可以提出行政复议。[45]

美国国家标准和技术研究院于 2014 年 2 月 12 日发布了 1.0 版的《网络安全框架》,该框架包括:一组用以预测和防护网络攻击的常见活动(“框架核心”),确定了关键基础设施保护应具有识别、保护、检测、响应和恢复等五种功能;一种用以评估核心活动实现程

---

〔42〕 The White House, *National Strategy for the Physical Protection of Critical Infrastructure and Key Assets*, February, 2003, http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf, pp. 71 - 79, last visited on Jul. 29, 2016.

〔43〕 National Infrastructure Simulation and Analysis Center,该中心是根据《2001 年关键基础设施保护法》而建立的。

〔44〕 E. O. 13636, Sec. 7 - 8.

〔45〕 Sec. 9, E. O. 13636.

度和测算应对攻击准备程度的分层方法(“框架实施层”),根据框架执行情况分为部分具备、熟知风险、符合标准和自动适应等四个层级;以及一个根据各组织业务需求、风险承受能力和资源确定的实施方案(“框架配套方案”),比较当前配套方案和目标配套方案,可以暴露问题,提升组织的网络风险管理。该框架还包括了一份较为全面的参考资料,列出了关键基础设施各个行业通用的一些特定标准、指南和实践。[46]

三 关于完善我国关键基础设施保护立法的建议

关键基础设施保护就是要保护关键基础设施所依赖的网络信息系统及其所存储和传输的数据不受非法行为的威胁和侵害。本文认为保护关键基础设施的基本策略,可以从如何应对其面临的威胁、漏洞和危害三大风险入手思考,主要应包括预防威胁、填补漏洞、应急恢复和信息共享四个方面。根据这四大基本策略,结合前述域外经验,本文提出以下我国关键基础设施保护的宏观立法思路,并针对我国《网络安全法(草案二审稿)》的相关条文,提出完善我国关键基础设施保护具体制度设计的建议。

(一)从国家安全高度把握关键基础设施的界定和立法

关键基础设施涉及能源、电力、通信、金融、交通以及政府服务等社会生活的重要领域,但是“关键基础设施”并不等同于“重要领域信息系统”,《国家安全法》第 25 条也是将二者并列表述。本文认为确定关键基础设施的内涵外延和立法体系,应该从国家安全的高度予以把握。

1. 关键基础设施的“关键”是指事关国家安全、公共安全

从各国关键基础设施保护立法来看,所谓的“关键”就是指事关国家安全和公共安全,这既突出了立法保护的重点,也可以将小企业和商业性信息技术产品排除在外,避免设立过多的监管义务而增加产业界的负担。二审稿第 29 条明确规定关键基础设施是指“一旦遭到破坏、丧失功能或者数据泄露,严重危害国家安全、国计民生、公共利益”的基础设施,相较于一审稿第 25 条定义采用的重要行业、公共服务、军事、政务、用户数量众多等不同标准,是重大进步。这和习总书记“4.19”重要讲话强调关键基础设施是“经济社会运行神经中枢”的论断相符合。这一定义将网络安全和关键基础设施保护立法提升到国家安全和公共安全的高度,不仅有利于突出保护重点,也有利于统筹安排关键基础设施保护的立法体系。对于不涉及国家安全和公共安全的问题,不宜规定在《网络安全法》之中,可以通过其他法律予以解决。

需要指出的是,草案一审稿和二审稿都采用了“关键信息基础设施”的表述,而《国家安全法》第 25 条规定保护“关键基础设施和重要领域信息系统”,采用的是“关键基础设施”的表述。本文建议采用“关键基础设施”的表述,理由如下:从问题本源看,关键基础

〔46〕 National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (*Version 1.0*), February 12, 2014, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf, last visited on Jul.29, 2016.

设施不仅面临物理威胁,也面临该设施信息系统部分遭受攻击的网络威胁,因此保护关键基础设施包括保护设施的物理部分和网络部分。有学者指出,“关键信息基础设施”概念就是强调保护设施的网络部分,但是这种理解和这个词的一般语义不符。从这个词看,其就是指关键的信息基础设施,而信息基础设施主要涉及电信业和信息技术业领域,国外就是在两个领域使用“关键信息基础设施”(CIIP)的概念。

从我国立法目的看,《国家安全法》的规定表明我国立法是要保护能源、交通、水利、金融等所有领域的关键基础设施。而“关键信息基础设施”这一表述,容易让人误解我国只保护电信业和信息技术业的关键基础设施,这和我国保护所有领域关键基础设施的立法目的不符。从国外立法例来看,美国、德国等国立法都采用的是“关键基础设施”的表述,“关键信息基础设施”不符合国外“关键基础设施”这一常用表述。如执意采用“关键信息基础设施”的概念,很可能造成交流上的障碍。比如很难说核电站是关键信息基础设施,而说核电站属于关键基础设施则不存在这一问题。

因此,本文建议将草案二审稿中的“关键信息基础设施”改为“关键基础设施”。如果强调立法只涉及保护关键基础设施的网络部分,而不涉及物理部分的防护,可采用“关键基础设施信息系统”的表述,而不应采用“关键信息基础设施”的表述。

2. 从国家安全、公共安全的高度进行立法的体系化设计

网络安全立法涉及了社会日常生活的多个领域,包括网络犯罪、技术标准、内容管制、电子政务、隐私权保护等等,内容多样复杂,需要战略性的布局和体系化的设计。确定网络安全立法重点的基本指导原则就是确保国家安全、公共安全,也就是说立法应关注网络信息系统及其所存储和传输的数据受到威胁和侵害时所引发的国家安全、公共安全问题。从美国、欧盟等国家的立法设想看,立法的核心就是关键基础设施保护,而关键基础设施保护立法体系本身也要在国家安全、公共安全的高度上把握设计。

应该承认关键基础设施保护法制是一个多层次规范相互配合的法律体系,而网络安全专门性立法应该着重解决其中事关国家安全的重点问题,面面俱到有可能导致重点不明、成效有限。有些问题应该通过其他法律规范来解决,不建议在《网络安全法》中规定。比如二审稿第三章第 26 条禁止网络非法侵入,重复了《刑法》第 285 条、第 286 条的规定,本文认为对于一般网络信息系统侵入行为的规制,在刑法里规定比较恰当。当然,第 285 条、第 286 条本身规定在“妨害社会管理秩序罪”之下,并没有认识到网络非法侵入犯罪可能危害公共安全的情形。针对社会生活的发展变化,建议我国刑法应该适时作出调整,将严重的网络非法侵入犯罪纳入“危害公共安全罪”,增大惩处力度。

此外,建议删去二审稿的第二章“网络安全支持与促进”,包括二审稿新增的第 16 条“国家推进网络安全社会化服务体系建设”和第 17 条“国家鼓励开发网络数据安全保护和利用技术”。[47] 这不是否定战略的重要性,相反国家网络安全战略极其重要。但从域外经验看,一般是先制定国家网络安全战略,再推进网络安全综合性立法。遗憾的是,虽然有关部门努力多年,我国至今没有国家网络安全战略。建议在这次立法进程中适时制

〔47〕 第 17 条本身和第 15 条有一定的语义重复。

定公布这一战略,以保持战略适度公开透明,防止其他国家战略误判。战略构想可以通过立法的具体制度设计来体现,但写成法条形式的必要性并不充分,战略构想本身很难成为具有规范效力的法律规定。2016 年 6 月 6 日,网信办、教育部等六部门联合发布《关于加强网络安全学科建设和人才培养的意见》,对加强网络安全学科建设和人才培养作出重大部署,受到广泛好评。二审稿第二章的内容写成此类战略政策文件较为妥当,不宜直接规定为法条。

(二)坚持国内经验总结与国外经验借鉴相结合原则

我国网络安全工作积累了不少工作经验,在关键基础设施立法中既要借鉴国外先进经验,也要立足国情总结国内经验,坚持二者相结合相协调。

1. 将“运行安全”、“信息安全”改为“系统安全”、“内容安全”

我国传统上对于网络安全的理解,包括网络系统安全(包括数据传输安全)和网络内容安全。网络信息系统中传输的数据信息所负载的内容,如果涉及敌视我国的价值观和意识形态,同样会影响我们的国家安全和社会稳定,网络内容管理是我国网络安全立法不应忽视的重要方面。[48] 二审稿第 3 章和第 4 章分别规定“网络运行安全”和“网络信息安全”,将关键基础设施保护规定在“网络运行安全”之下。但“运行安全”和“信息安全”的划分并不妥当:一方面,关键基础设施保护强调的系统安全,其实包括系统中传输的数据安全,而“信息安全”的语义可以包括“数据安全”,那么关键基础设施保护的相关内容也应写入第 4 章;另一方面,第 4 章“信息安全”里规定的个人信息收集、传输、利用其实也属于“运行安全”,而且在“信息安全”这个“大概念”之下却只有个人信息保护的内容,并没有涉及内容管理,和我国对网络安全、信息安全的传统理解不符。

建议将第 3 章和第 4 章的章名改为“网络系统安全”和“网络内容安全”:将保护关键基础设施和一般信息系统的规定,包括确保数据传输安全的规定纳入第 3 章“网络系统安全”;充实第 4 章“网络内容安全”的规定,可以考虑增加未成年人上网保护的规定,以及网络内容管理的规定,包括实名制、内容分级制、信息删除规范等。对于二审稿第四章“网络信息安全”第 39 - 44 条对个人信息的保护,考虑到《刑法》《消费者权益保护法》等已经有了类似规定,而且还有专门制定个人信息保护法的主张,个人信息保护本身也不是网络信息系统受到侵害会引发的国家安全、公共安全的主要问题,没有必要规定如此详细,建议只规定一条,该条可以考虑改造二审稿第 21 条第 3 款而表述为:“网络产品、服务具有收集用户信息功能的,其提供者应当向用户明示并取得同意;收集公民个人信息的,应当遵守有关法律、行政法规关于公民个人信息保护的规定。”

需要指出的是,规定“网络内容安全”,不仅有利于规范我国网络内容管理秩序,也有利于以法律武器维护网络空间主权,反击他国以“互联网自由”之名干涉我国内政。奥巴马政府在《网络空间国际战略》中宣扬“互联网自由”,美国国务卿希拉里·克林顿也在演讲中多次强调“网络自由”,公开宣称“我们投资开发尖端技术,因为我们知道压制性政府

〔48〕 参见刘金瑞:《三网融合下视听媒体内容管制对策》,《中国电信业》2011 年第 3 期,第 60 - 62 页。

不停地翻新钳制手段,而我们必须走在他们前面”。[49] 促进信息自由流动确实是互联网的崇高价值,但是一国政府按照自设标准去判定其他国家的政策立法是正常管制还是过度“钳制”则不无疑问,一国政府利用自身技术优势对其他国家网络监管进行干涉的国际法基础并不存在。我们不仅应警惕网络技术层面的网络系统安全威胁,也要警惕其他国家利用技术优势传播敌对言论而引发的网络内容安全威胁。

2. 处理好关键基础设施保护和信息安全等级保护的关系

我国长期以来对信息系统的管理实行“信息安全等级保护管理制度”,这体现在二审稿第三章“网络运行安全”第一节“一般规定”的第 20 条(条文称之为“网络安全等级保护制度”)。但草案中还借鉴了国外的“关键基础设施保护”制度,规定在草案第三章“网络运行安全”第二节“关键信息基础设施的运行安全”。相较于一审稿,二审稿在第 29 条明确规定“在网络安全等级保护制度的基础上”,对关键基础设施“实行重点保护”。从这一条规定看,好像是将关键基础设施保护纳入到网络安全等级保护里最为重要的部分。但二审稿中,两部分的内容仍有很多重复之处,比如第 21、22 条和第 33、34 条,都是为了确保供应链安全。这需要清楚界定二者的适用范围,应进一步协调这两个制度的关系和分工。二审稿从国家安全的角度界定了关键基础设施,那么关键基础设施保护制度应适用事关国家安全和国家命脉的基础设施。而对于等级保护管理制度,以“自主定级、自主保护”为原则,应进一步明确适用于所有一般网络信息系统。

可以将关键基础设施规定为最高等级的网络信息系统或其中之一部分,但关键基础设施的保护范围和强制性监管标准,应该规定国家网信部门按照法定授权予以确定制定。从域外经验看,无论是美国还是欧盟,虽然公开关键基础设施涉及的重要行业领域,但具体的关键基础设施列表清单是秘密的。换言之,关键基础设施的具体范围是秘密的。这个很容理解,既然关键基础设施涉及国家安全、公共安全,一旦公开关键基础设施清单,那就会成为敌对势力和恐怖分子的攻击目标,后果不堪设想。从这个意义上讲,二审稿第 29 条第 1 款最后一句“关键信息基础设施的具体范围和安全保护办法由国务院制定”并不妥当,我国也应该实行关键基础设施秘密保护制度,建议规定:“关键基础设施的安全保护办法由国务院制定”,而“关键基础设施的具体范围由国家网信部门按照法定授权予以认定;国家网信部门负责组织制定关键基础设施保护国家计划、行业计划和强制性监管标准;国家网信部门应秘密通知关键基础设施的所有者或运营者,要求其遵守国家强制性监管标准,并对其是否遵守标准的情况予以监督核查”。

(三)设计监管框架时区分一般和关键、公共和私营

网络信息系统涉及社会生活的不同部门和各个领域,在设计监管框架时应有所区分,既有利于根据不同情况设定妥当的监管标准,也有利于不同主体明确自身的权利义务,本文建议关键基础设施保护和网络安全立法做到以下两个区分。

1. 区分一般信息系统和关键基础设施设定不同的保护

从域外经验看,往往对关键基础设施和一般信息系统设定不同的保护标准,对于关键

〔49〕 Hillary Clinton, *Internet Rights and Wrongs: Choices & Challenges in a Networked World*, http://www.state.gov/secretary/rm/2011/02/156619.htm, last visited on Jul. 29, 2016.

基础设施而言,除了得到普通信息系统的一般保护之外,还应给予其特别保护。二审稿第一节“一般规定”和第二节“关键信息基础设施的运行安全”,没有区分信息系统的一般保护和关键基础设施的特别保护,导致这两节中有些内容缺乏规定而有些内容存在交叉,比如第二节第 32 条规定的关键基础设施运营者应履行的“教育从业人员”、“容灾备份”、“制定网络安全事件应急预案”等义务,同样是其他信息系统一般保护所需要的。建议将第 3 章第一节“一般规定”改为“信息系统的一般保护”,梳理二审稿适用于所有信息系统保护的运营者的义务(如漏洞报告、协助执法等)、监管部门的权限等,将这些内容规定于该节之下;将第 3 章第二节改为“关键基础设施的特别保护”,只纳入适用关键基础设施的特别规定。

值得讨论的是,二审稿第 35 条规定的“数据境内存储”到底属于信息系统的一般保护义务还是关键基础设施的特别保护义务。本文认为,这涉及“数据境内存储”的定位问题。如果认为其定位是便于本国政府监管尤其是便于执法时追查证据和追踪犯罪,那么应该作为信息系统的一般义务,规定在本文认为的第 3 章第一节“信息系统的一般保护”,相应地义务主体应该改为“信息系统的运营者”。但如果认为其定位是为了维护关键基础设施所涉及的国家安全和公共安全,那么应该规定在本文认为的第二节“关键基础设施的特别保护”。二审稿条文的问题在于,既然规定义务主体是关键基础设施运营者,那么就事关国家安全和公共安全,既然如此重要,为何还规定可以向“境外提供”?虽然该条规定了评估程序,可由前文所述,对关键基础设施应采用秘密保护制度,这种评估程序反而可能会暴露关键基础设施而让其陷入更大的风险之中。本文建议,如果将“数据境内存储”义务认为是关键基础设施的特别保护义务,则规定其相关数据不能向境外传输。

2. 区分公共部门和私营部门设计不同的监管框架

二审稿并没有对公共部门和私营部门的网络信息系统进行区分保护,提供信息服务的政府网络基本可以纳入草案所定义的“网络经营者”的范围,而遵循与私营部门一样的网络安全义务。而公共部门的网络信息系统比一般私营部门更加重要,公共部门信息系统被攻击包括其传输的信息被篡改、窃取往往造成的危害更大,公共部门的关键基础设施保护更是重中之重,所以在监管标准、技术建设等方面都应不同于私营部门。美国早在 2002 年就通过了《联邦信息安全管理法》,并在 2014 年 12 月进行了修改,明确了各部门维护联邦网络安全的职责,授权了实时、自动监控联邦计算机网络,并大幅减少了安全审查中的文书工作量。美国在政府系统内部署“爱因斯坦”计划(入侵检测系统和入侵防御系统)以应对威胁,但对于大部分的私营关键基础设施来说,美国政府不可能强行将其纳入“爱因斯坦”检测防御系统,所以美国网络安全立法中的重点是“私营”关键基础设施的保护。习总书记在“4. 19”讲话中明确指出,“要落实网络安全责任制,制定网络安全标准,明确保护对象、保护层级、保护措施”,要明确由政府保障的方面和由市场力量防护的方面。建议二审稿针对公共部门和私营部门设立不同的监管框架,对于公共部门要规定采用统一的技术规范,要求其严格遵守统一的监管标准。

（四）监管私营部门要贯彻安全与发展并重的原则

坚持安全与发展并重是《网络安全法（草案）》起草说明中提到的基本原则，习总书记“4.19”讲话进一步指出“坚持鼓励支持和规范发展并行”。二审稿虽然增加了约谈、记入信用档案、从业禁止等惩戒措施，有利于督促企业履行义务，但私营关键基础设施应该遵循何种义务来实现安全的目标仍不明确。本文建议在坚持安全与发展并重的前提下增加如下规定，以完善私营关键基础设施的保护。

1. 明确监管标准的强制效力，但审慎划定私营关键基础设施的范围

从美国和欧盟的立法经验来看，综合性网络安全立法针对私营企业关键基础设施保护的规定主要是确定私营关键基础设施的范围并要求其遵守强制性的监管标准。二审稿第14条规定“国家建立和完善网络安全标准体系”，但并没有规定这些标准是否具有强制效力。如果这些标准是自愿遵守的，将无法实现强化相关私营主体责任，进而实现确保私营关键基础设施安全之目的。

建议增加以下规定：国家组织制定的网络安全标准具有强制效力，纳入关键基础设施范围的所有者或运营者应严格遵守有关的强制性标准；国家网信部门负责认定关键基础设施的网络安全威胁，指定哪些资产或系统属于关键基础设施，并协同国家有关部门为这些设施提供相应的监管方案和监管标准；纳入关键基础设施范围的系统或资产，必须遵守强制性监管要求，否则要承担相应的法律责任。考虑到强制性监管标准确实会给企业增加负担，应该审慎划定私营关键基础设施的范围，可以考虑借鉴前述德国和美国的规定，将“小企业”和“商业信息技术产品或消费信息技术服务”排除在外。

2. 构建政府和企业的协作机制，完善安全信息共享和企业责任豁免

关键基础设施保护的技术性较强，实现关键基础设施安全可控，离不开产业界的支持，政府不应该把企业只当作是被监管者，而是应该把企业当成是协作者，共同维护网络安全。二审稿缺乏授权政府与企业协作的规定；对于网络安全信息共享，只是在第37规定“促进网络安全信息共享”，新增第38条规定“国家网信部门和有关部门在关键信息基础设施保护中获取的信息，只能用于维护网络安全的需要，不得用于其他用途”，规定过于简单，没有具体负责机构和实现机制，对企业的激励也不够充分。建议增加授权政府与企业建立协作机制的规定，并完善网络安全信息共享和企业责任豁免制度。

一是授权国家网信部门、相关行业主管部门与私营关键基础设施运营者进行合作，制订专门的合作保护计划。在国家网络安全标准制订中，要广泛征求产业界的意见，充分反映行业的最佳实践。二是完善网络安全信息共享制度，健全政府和企业的网络安全信息共享机制和行业内网络安全信息共享机制。授权网信部门建立专门的网络安全信息共享国家中心；授权网信部门推动建立行业内部以及政府和行业之间的网络安全信息交换组织；规定共享的网络安全信息，免除信息公开的披露义务，不能侵害个人隐私、商业秘密和其他合法权益。三是规定企业在遵循法定强制标准和按照法定要求共享网络安全信息的情况下，免除因此而产生的法律责任。例如，对于遵守了强制性监管标准的关键基础设施所有者或运营者，在其信息系统被恶意攻击而导致大规模数据泄露时，可以考虑规定其不用向消费者承担惩罚性赔偿责任。

(五)在相关条文拟定中为国际规则制定留下适当空间

网络的互联互通和全球性,使得以保护关键基础设施为核心的网络安全问题成为当今世界各国共同面临的挑战。世界各国只有在共同参与、沟通合作的基础上,就网络安全规则达成共识,才能真正解决这一全球性的难题。为在将来国际规则制定中掌握主动,我国立法应从国际法角度设计一些必要的条款。

1. 通过完善管辖权条款确认法律的域外效力

二审稿第 2 条规定:"在中华人民共和国境内建设、运营、维护和使用网络,以及网络安全的监督管理,适用本法。"该条仅规定了法律的域内效力,并没有考虑法律的域外效力,不利于维护我国的国家安全和网络空间主权。建议参照我国《刑法》相关条文的规定,除了"属地管辖权"之外,还要规定"属人管辖权"、"保护管辖权"和"普遍管辖权"。对于普遍管辖权,可以拟定如下条文:"对于中华人民共和国缔结或者参加的国际条约所规定的网络安全犯罪行为,中华人民共和国在所承担条约义务的范围内行使管辖权的,适用本法。"在网络空间谋求绝对安全几乎是不可能的,我国未来应该积极主导、参与网络安全国际规则的制定,起草相关国际条约,通过国际合作来实现各国网络空间真正的普遍安全,而管辖权规定也为这些战略设想留有空间。

2. 原则上规定针对网络攻击的反制措施

当前,跨国网络攻击日益频繁,针对我国关键基础设施和重要信息系统的 APT 攻击、漏洞后门攻击呈逐年上升的趋势,我国已经成为网络攻击的主要受害国。除了加大科研力度,对网络攻击予以技术防范和应对之外,也应该考虑从法律上规定针对网络攻击的反制措施。对此,美国已经有类似规定。奥巴马政府于 2015 年 4 月颁行《第 13694 号行政命令》(E. O. 13694),宣布将针对美国实施恶意网络活动的主体予以制裁。所谓的恶意网络活动包括以下情形:显著破坏了美国关键基础设施;盗窃美国经济资源、商业秘密、个人身份信息或者金融信息以获得商业竞争优势、个人经济利益;接受或使用窃取的商业秘密而从中获益;破坏美国计算机网络或者为上述活动提供物质支持。这些恶意网络活动会造成美国国家安全、外交政策、经济安全和金融稳定面临"显著"威胁。根据这一命令,针对实施恶意网络活动的个人和实体,美国财政部长在与国务卿、司法部长协商的基础上,可以对这些个人或实体采取以下措施:冻结其资产、禁止其进入美国、禁止其与美国公民或公司进行商业往来。[50]

我国与俄罗斯等国向联合国提交的《信息安全国际行为准则》(2015 年版草案),主张"各国有责任和权利依法保护本国信息空间及关键信息基础设施免受威胁、干扰和攻击破坏","任何争端,都以和平方式解决,不得使用武力或以武力相威胁"。[51] 规定合理的反制措施,并非是诉诸武力解决争端,而是一国维护自身关键基础设施安全的必要手段。本文建议在二审稿中原则上规定针对网络攻击的反制措施,条文可拟定为:"国家有

---

〔50〕 E. O. 13694: Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities, Federal Register, Vol. 80, No. 63, April 2, 2015, pp. 180747 - 18079.

〔51〕 《信息安全国际行为准则》, http://infogate.fmprc.gov.cn/web/ziliao_674904/tytj_674911/zcwj_674915/P020150316571763224632.pdf,最后访问日期:2016 年 7 月 29 日。

权针对境内外的网络安全攻击采取反制措施,包括但不限于技术反击和经济制裁。”至于具体适用条件和程序需要严格限制,可以在今后的实践中逐渐确立细化。虽然这一规定是原则性的,但可以对有关网络攻击方形成一定的威慑,也有利于今后我国在网络安全国际规则制定中掌握一定的主动权。

[本文为中央马克思主义理论研究和建设工程重大项目、国家社科基金重大项目“全面推进依法治国重大现实问题研究”(2015MZD042)和国家社会科学基金特别委托项目“大数据时代依法治国战略”(15@ ZH012)的研究成果。]

[**Abstract**] The protection of critical infrastructure (CI) has been the core issue of governance and legislation on cyberspace all over the world. Foreign legislations in this field, represented by that of the United States, focus on the protection of private CI and cyber security information sharing. The current institutional framework of policy implementation of CI protection in the United States has the follow components: government-sector coordination; national CI protection plan; information sharing and analysis center; identification of CI, assessment of vulnerability and risk, and prioritization of protective measures; and cyber security framework. Based on foreign experiences, this author puts forward the following proposals on CI legislation in China: treating the definition of CI and the systematization of the relevant legislations as matters of national security; adhering to the combination of domestic practices and foreign experiences, dividing cyber security into system security and content security, and properly deal with the relationship between CI protection and multi-level protection of information security; designing the regulatory framework on basis of distinguishing between common information system and CI and between public sector and private sector; attaching equal importance to security and development in regulating the private sector, establishing a mechanism for the coordination between the government and enterprises, and improving the cyber security information sharing system and the system of exemption of private business from responsibilities; providing for the extraterritorial effect of the relevant laws and countermeasures against cyber attack, so as to leave room for the development of international regulations in future.

(责任编辑:支振锋)