理论前沿

“以管理为基础的规制”

——对网络运营者安全保护义务的重构

洪延青

内容提要:和世界上大多数国家一样,我国的网络运营者主要是党政军和国有企事业单位之外的私营部门。因此,如何妥善地界定他们所需承担的网络安全保护义务,是改善我国网络安全状况的关键问题之一。在此方面,现行制度和两次公开征求意见的《网络安全法(草案)》,均采用了“关注安全底线的、静态的、具体的措施性规定”,作为网络运营者安全保护义务的核心内容。而在网络安全形势瞬息万变的今天,“关注安全底线的、静态的、具体的措施性规定”实际上并不足以为网络和信息系统提供实质性的安全。因此,《网络安全法》中对于安全保护义务的制度设计,应该致力于让网络运营者在内部决策环节就足够重视风险管理,使安全义务从外部“至上而下”地施加转变为“内化于心”。

关键词:网络安全　网络运营者　安全保护义务　以管理为基础的规制

洪延青,荷兰乌特勒支大学法学博士。

目前,我国网络安全形势不容乐观:据国家互联网应急中心(CNCERT)发布的《2014年我国互联网网络安全态势报告》,中国数据信息保护正面临严峻挑战。仅2014年,中国就有多家知名电商、快递公司、招聘网站、考试报名网站等发生数据泄露事件;2014年5月,某知名手机厂商论坛数据泄露,由于用户管理模块存在漏洞,导致包括账号、密码和社交账号等800万用户个人信息泄露。[1] 最新发布的《2015年我国互联网网络安全态势综述》显示,2015年,我国同样发生了严重的数据泄露事件:约10万条应届高考考生信息泄露事件、某票务系统近600万用户信息泄露事件等等。[2]

〔1〕 国家计算机网络应急技术处理协调中心著:《2014年我国互联网网络安全态势报告》,http://www.cert.org.cn/publish/main/12/2015/20150430151528629942561/20150430151528629942561_.html,最后访问日期:2016年7月13日。

〔2〕 国家互联网应急中心:《2015年我国互联网网络安全态势报告》,http://www.cert.org.cn/publish/main/12/2016/20160422085056915532001/20160422085056915532001_.html,最后访问日期:2016年7月17日。

当然,数据泄露并非我国一家独有。美国智库对外关系委员会将2014年评为“商业网络攻击的一年”。2014年,除针对索尼影业的网络攻击外,美国还发生数起“千万级”的数据泄露事件,造成了不可估量的经济损失,如2014年1月,著名零售公司Target宣布黑客窃取了超过7000万顾客包括姓名、地址等在内的个人信息,以及4000万张信用卡的数据;2014年8月,摩根大通银行承认,在其遭受的网络攻击中,7600万家庭用户和700万小型企业的信息被泄露,涉及人数超过美国人口的四分之一。[3]

毫不夸张地说,当下国内外一起起数据泄露事件正在“抢着上头条”。在数字经济时代,数据的重要性无需赘述。其中,个人信息因“能够单独或者与其他信息结合识别用户”[4],更是“价值堪比石油和黄金”。反过来,数据泄露也给这些企业带来巨大的负担。根据IBM和美国数据安全保护权威研究机构Ponemon Institute于2016年发布的报告,2016年数据泄露事故中每条记录的成本达到158美元,单起数据泄露事故的平均总成本高达400万美元。[5]可以说,数据泄露等网络安全事件频发,已经成为任何使用计算机和互联网的单位、个人都无法回避的问题。

2015年7月6日,全国人大公布了《中华人民共和国网络安全法(草案)》,向社会公开征求意见。[6] 2016年7月6日,全国人大又公布了《中华人民共和国网络安全法(草案)》(二次审议稿)。[7] 作为网络安全领域最重要的立法,《网络安全法(草案)》对网络运营者[8]的安全保护义务做出明确规定。一审稿的立法说明指出,“保障网络运行安全,必须落实网络运营者第一责任人的责任”[9],清晰明确地规定了网络运营者是保护网络安全和个人信息的主要责任人。而在确定责任主体后,《网络安全法(草案)》和现行制度对网络运营者安全保护义务内容的规定是否充分、能否达到效果,就成为改善、保障我国网络安全最重要的问题之一。如果不足,又该如何改进?和世界上大多数国家一样,我国的网络建设、运营方主要是党政军和国有企事业单位之外的私营部门。在网络安全保护上,党政军和国有企事业单位所承担的义务也与私营部门有所不同,[10]本文将主要关注

〔3〕 Council on Foreign Relations, “The Top Five Cyber Policy Developments of 2014: A Year of Corporate Cyberattacks”, Dec 30, 2014, http://blogs.cfr.org/cyber/2014/12/30/the-top-five-cyber-policy-developments-of-2014-a-year-of-corporate-cyberattacks/, 最后访问日期:2016年6月1日。

〔4〕 《电信和互联网用户个人信息保护规定》第四条。

〔5〕 Ponemon Institute and IBM, “2016 Ponemon Cost of Data Breach Study”, http://www-03.ibm.com/security/data-breach/ 在该报告中,Ponemon Institute对12个国家的383个遭受数据泄露的公司进行了分析:成本中除了公司为数据遭泄露的主体提供各种降低风险服务的费用外,还包括公司的业务损失、客户流失、声誉和商誉受损等。最后访问日期:2016年7月17日。

〔6〕 “网络安全法(草案)全文”,http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm,最后访问日期:2016年6月1日。

〔7〕 “网络安全法(草案二次审议稿)全文”,http://www.npc.gov.cn/npc/flcazqyj/2016-07/05/content_1993343.htm,最后访问日期:2016年7月13日。

〔8〕 按照《网络安全法(草案)》的定义,网络运营者,是指网络的所有者、管理者以及利用他人所有或者管理的网络提供相关服务的网络服务提供者,包括基础电信运营者、网络信息服务提供者、重要信息系统运营者等。现行法律法规对此使用了不同的概念,但本文将统一采用“网络运营者”概念。

〔9〕 见一审稿立法说明,http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm,最后访问日期:2016年7月18日。

〔10〕 关于党政军和国有企事业单位承担的网络安全保护义务的部分规定涉密,没有公开。

私营部门的网络安全保护义务。

对比《网络安全法(草案)》一审和二审稿文本,对网络运营者安全保护义务的主要规定仅有略微变化,可见立法者延续了网络运营者安全保护义务的立法思路。因此,如无特别说明,下文将主要引用《网络安全法(草案)》(二审稿)的文本。

一 网络运营者的安全保护义务——中国的逻辑

保障我国网络安全,核心问题之一是"如何让私营部门动起来",切实做到"守土有责"、"守土负责"、"守土尽责"。其中首要问题是把"责"规定好。

(一)网络安全和数据保护的责任主体——"谁运营谁负责"

按照现行规定,网络安全和数据保护的责任主体是网络运营者。"谁运营谁负责"是一个简明的概括。例如,在法律层面,全国人大常委会《关于加强网络信息保护的决定》第四条规定,"网络服务提供者和其他企业事业单位应当采取技术措施和其他必要措施,确保信息安全,防止在业务活动中收集的公民个人电子信息泄露、毁损、丢失。在发生或者可能发生信息泄露、毁损、丢失的情况时,应当立即采取补救措施。"

在法规层面,《中华人民共和国计算机信息系统安全保护条例》第十三条规定,计算机信息系统的使用单位应当建立健全安全管理制度,负责本单位计算机信息系统的安全保护工作;《中华人民共和国电信条例》第五十九条规定,电信业务经营者应当按照国家有关电信安全的规定,建立健全内部安全保障制度,实行安全保障责任制。[11]

综合《网络安全法(草案)》第十条[12]和立法说明[13]的内容,可以看出草案也遵循了"谁运营谁负责"的理念:"建设、运营网络或者通过网络提供服务"的一方承担主要的安全保护义务,政府部门更多的是协调、监督、管理。[14] 换句话说,《网络安全法(草案)》对"建设、运营网络或者通过网络提供服务"的一方施加了安全保护义务,政府将主要监管这些义务是否履行到位和充分。

(二)安全保护义务的主要内容

1.《网络安全法(草案)》

目前《网络安全法(草案)》对"责"的主要规定体现在第十条、第十四条、第二十条中,网络安全等级保护制度是网络安全保护的基本制度;同时国务院标准化行政主管部门

---

〔11〕 规章层面更加明确地体现了"谁运营谁负责"的思路。公安部《计算机信息网络国际联网安全保护管理办法》第十条规定:"互联单位、接入单位及使用计算机信息网络国际联网的法人和其他组织应当履行安全保护职责。"工信部《电信和互联网用户个人信息保护规定》第六条规定:"电信业务经营者、互联网信息服务提供者对其在提供服务过程中收集、使用的用户个人信息的安全负责。"

〔12〕 该条规定:"建设、运营网络或者通过网络提供服务,应当依照法律、法规的规定和国家标准的强制性要求,采取技术措施和其他必要措施,保障网络安全、稳定运行,有效应对网络安全事件,防范网络违法犯罪活动,维护网络数据的完整性、保密性和可用性。"

〔13〕 见一审稿立法说明,http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm,最后访问日期:2016 年 7 月 18 日。

〔14〕 政府部门针对特定对象,还承担部分安全保护的职责,但不在本文讨论的范围内。

和国务院有关部门组织制定网络安全相关的国家标准、行业标准;网络建设、运营方按照网络安全等级保护制度的要求和国家标准、行业标准的强制性要求,采取相应的管理措施、技术防范及其他必要措施。

也就是说,网络运营者安全保护义务的“责”,主要来自于三部分:一是网络安全等级保护制度;二是国家标准、行业标准(两者共同规定了管理措施和技术措施的内容);三是“其他必要措施”。这一点也明确体现在《网络安全法(草案)》第四十一条对网络运营者维护信息安全的规定中:“网络运营者应当采取技术措施和其他必要措施,确保公民个人信息安全,防止其收集的公民个人信息泄露、毁损、丢失。”《网络安全法(草案)》在第三十二条还对关键信息基础设施的安全保护义务做出了额外规定,同样遵循了上述逻辑。

2. 网络安全等级保护制度(信息安全等级保护制度)

在公布一审稿时,全国人大常委会法工委对“网络安全等级保护制度”做出如下立法说明:“草案将现行的网络安全等级保护制度上升为法律,要求网络运营者按照网络安全等级保护制度的要求,采取相应的管理措施和技术防范等措施,履行相应的网络安全保护义务。”[15]值得注意的是,我国现行的是“信息安全等级保护制度”,并没有所谓的“网络安全等级保护制度”。笔者推测,并非法工委犯了错误,而是为了在网络安全立法中保持概念上的一致。因此可以认为,草案中的“网络安全等级保护制度”将沿袭现行的“信息安全等级保护制度”。

在现行体制中,信息安全等级保护在国家信息安全保障体系中是一项基本制度”,是指“对国家秘密信息、法人和其他组织及公民的专有信息以及公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护,对信息系统中使用的信息安全产品实行按等级管理,对信息系统中发生的信息安全事件分等级响应、处置”。[16]

信息安全等级保护的核心是对信息系统分等级、按标准进行建设、管理和监督(见图一)。分级的依据是“信息系统在国家安全、经济建设、社会生活中的重要程度,信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素”。[17]

总的来说,信息安全等级保护的基本逻辑是:(一)针对不同等级,制定相应的管理规范和技术标准;(二)根据信息和信息系统的不同重要程度,以及每一等级的管理规范和技术标准,组织行政机关、公民、法人和其他组织开展有针对性的保护工作;(三)政府对不同安全保护级别的信息和信息系统实行不同强度的监管政策。因此,在信息安全等级保护制度中,不同分级配套的管理规范和技术标准构成了安全保护义务的主要内容。

3. 信息安全等级保护国家标准、行业标准的内容和特征

《网络安全法(草案)》中,“国家标准、行业标准”贯穿于安全保护义务的有关条文。

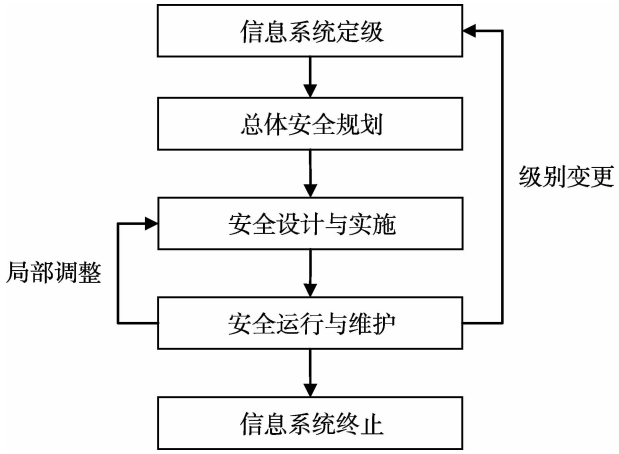
---

〔15〕 “网络安全法(草案)全文”,http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm,最后访问日期:2016年6月1日。

〔16〕 张伟丽:《信息安全等级保护现状浅析》,《信息安全与技术》2014年第9期,第10页。

〔17〕 《信息安全等级保护管理办法》第六条。现行体制中,信息系统的安全保护等级共分五级:自主保护级(第一级)、指导保护级(第二级)、监督保护级(第三级)、强制保护级(第四级)、专控保护级(第五级)。

图一:信息系统安全等级保护实施的基本流程



信息安全等级保护制度则采用了“管理规范和技术标准”的表述。根据全国人大法工委的立法说明,可以认为“国家标准、行业标准”与“管理规范和技术标准”具备相同内涵。信息安全等级保护制度涉及众多国家标准。[18] 这里的分析将以系统定级和建设中涉及的标准为主,原因是系统定级是实施信息系统安全等级保护的前提和基础,而定级后不同安全保护等级信息系统的基本保护要求,则规定了安全保护义务的主要内容。

(1)标准的内涵

从本质上讲,标准是对重复性事物和概念所做的统一规定。它以科学、技术和实践经验的综合成果为基础,经有关方面协商一致,由主管机构批准,以特定形式发布,作为共同遵守的准则和依据。[19] 而信息安全标准是确保信息安全的产品和系统在设计、研发、生产、建设、使用、测评中解决其一致性、可靠性、可控性、先进性和符合性的技术规范、技术依据。[20]

(2)定级标准

《信息系统安全保护等级定级指南》规定,“信息系统的安全保护等级由两个定级要素决定:等级保护对象受到破坏时所侵害的客体和对客体造成侵害的程度。”其中客体是指“受法律保护的、等级保护对象受到破坏时所侵害的社会关系,如国家安全、社会秩序、公共利益以及公民、法人或其他组织的合法权益”。上述逻辑可用图二直观表示:[21]

〔18〕 具体来说,(一)基础标准:《计算机信息系统安全保护等级划分准则》(GB17859 - 1999)、《信息系统安全等级保护实施指南》(GB/T 25058 - 2010);(二)系统定级环节:《信息系统安全保护等级定级指南》(GB/T22240 - 2008);(三)建设、整改环节:《信息系统安全等级保护基本要求》(GB/T22239 - 2008);(四)等级测评环节:《信息系统安全等级保护测评要求》(GB/T28448 - 2012)、《信息系统安全等级保护测评过程指南》(GB/T28449 - 2012)。

〔19〕 高林:《标准化工作有力支撑网络安全保障》,《信息安全与通信保密》2014 年第 12 期,第 49 页。

〔20〕 林宁、吴志刚:《我国信息安全标准化概况》,《信息技术与标准化》2006 年第 8 期,第 59 页。

〔21〕 第一级,信息系统受到破坏后,会对公民、法人和其他组织的合法权益造成损害,但不损害国家安全、社会秩序和公共利益。第二级,信息系统受到破坏后,会对公民、法人和其他组织的合法权益造成严重损害,或者对社会秩序和公共利益造成损害,但不损害国家安全。第三级,信息系统受到破坏后,会对社会秩序和公共利益造成严重损害,或者对国家安全造成损害。第四级,信息系统受到破坏后,会对社会秩序和公共利益造成特别严重损害,或者对国家安全造成严重损害。第五级,信息系统受到破坏后,会对国家安全造成特别严重损害。

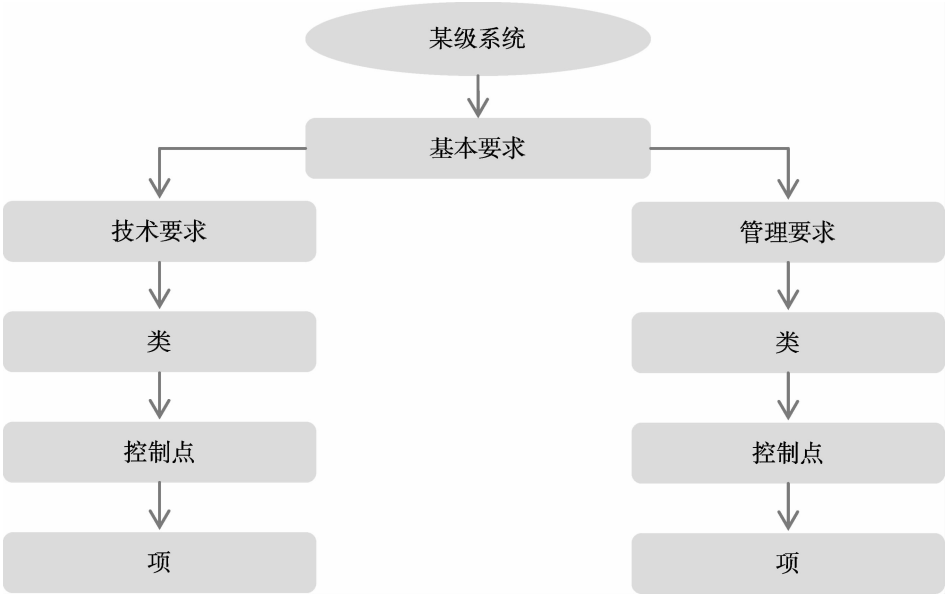
图二:信息系统等级划分示意

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

(3)基本安全保护能力

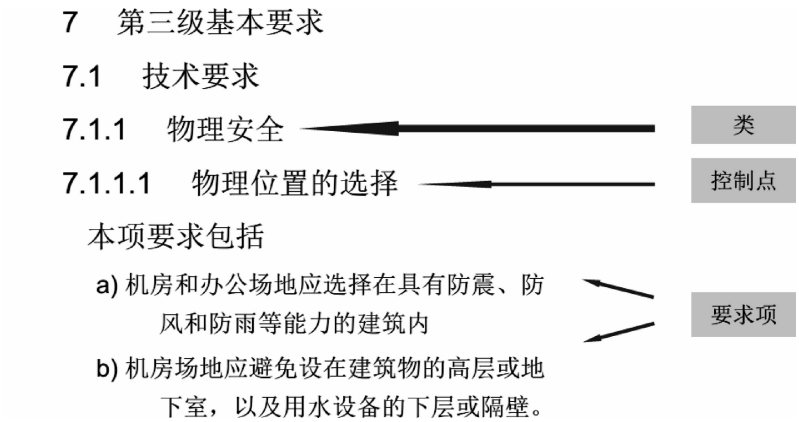
《信息系统安全保护等级定级指南》规定,网络运营者应当保证系统具有相应等级的基本安全保护能力,不同安全保护等级的信息系统要求具有不同的安全保护能力。因此,系统完成定级后,就需根据《信息系统安全等级保护基本要求》进行建设。在该标准中,安全保护能力是指“系统能够抵御威胁、发现安全事件以及在系统遭到损害后能够恢复先前状态等的程度”。《信息系统安全等级保护基本要求》详细阐述了各级的安全保护能力目标,并把如何实现各级的安全保护能力进行了具体分解(见图三)。

图三:信息系统安全等级保护要求分解图



其中类[22]、控制点、项的内容具体见下面的例子:

〔22〕 基本技术要求的类,包括物理安全、网络安全、主机安全、应用安全和数据安全;基本管理要求的类,包括安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理。



综上,《信息系统安全等级保护基本要求》的基本逻辑是,分级别规定不同的类、控制点、要求项,如果做到了这些类、点、项的要求,基本就可以认为该系统达到了某一特定安全保护能力的目标。

(4)行业标准

电力与银行、证券、海关、铁道、民航、税务被确定为七个重点行业信息安全领域。[23] 这些行业的安全标准基本是在《信息系统安全等级保护基本要求》的基础上,根据各自行业的特点进行一定程度的扩展。[24] 例如,国家电网在国家标准基础上进行深化、扩充,将二级系统技术要求项由 79 个扩充至 134 个,三级系统技术要求项由 136 个扩充至 184 个,形成了企业信息系统安全等级保护要求。[25]

综上,信息安全等级保护相关的国家标准、行业标准,在规定网络运营者的安全保护义务时遵循了如下思路:首先,根据系统遭破坏后造成的后果的不同严重程度,设定了五类安全保护等级;其次,在每一类安全保护等级中,设定不同的技术和管理要求的类、控制点、项。因此,这些类、具体的控制点、具体的要求项的总和,就构成了网络运营者安全保护义务的主要内容。换句话说,在实际建设和运营网络时,只要把某一特定安全保护等级要求做到的所有"要求项"都列出来,然后一项项予以落实,就可认为履行了安全保护义务。

4. 国家公权力监管的强度

对不同安全保护级别的信息和信息系统,政府实行不同强度的监管政策。根据《关于信息安全等级保护工作的实施意见》,第一级,运营者自主保护;第二级,政府给予指导;第三级,政府要对履行义务情况进行监督和检查;第四级,政府要对履行义务情况进行强制监督和检查;第五级,政府将会指定专门部门、专门机构进行专门监督。《信息安全等级保护管理办法》第十八条要求对第三级信息系统每年至少检查一次,对第四级信息

〔23〕 王志强:《信息系统安全等级保护研究与实践》,《信息化建设》2011 年第 8 期,第 47 页。

〔24〕 "重点行业可以按照《基本要求》等国家标准,结合行业特点,在公安部等有关部门指导下,确定《基本要求》的具体指标,在不低于《基本要求》的情况下,结合系统安全保护的特殊需求,制定行业标准规范或细则,并据此开展安全建设整改工作。"郭启全:《加快落实信息安全等级保护整改建设工作》,《信息安全与通信保密》2010 年 5 期,第 21 页。

〔25〕 王志强:《信息系统安全等级保护研究与实践》,《信息化建设》2011 年第 8 期,第 48 页。

系统每半年至少检查一次,并进一步规定了政府检查的主要内容。从第十八条列举的检查内容来看,政府部门监管的主要目的是确保国家标准、行业标准列出的安全管理制度、技术措施落实到位。

5. 总结

由上可知,《网络安全法(草案)》对我国网络运营者的安全保护义务所采取的基本逻辑可以总结为:首先,划分安全保护等级;其次,分级配套不同的国家标准、行业标准作为强制性要求;再次,每一等级配套的国家标准、行业标准非常具体地规定安全管理制度和技术措施;最后以“其他必要措施”作为兜底条款。综合分析,草案中网络运营者的安全保护义务具有三个鲜明特征:

(1)以具体的措施性规定为主。这些安全保护的措施主要基于过往防护工作中被证明为行之有效的做法。例如,《信息系统安全等级保护基本要求》规定:“应在网络边界处监视以下攻击行为:端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等。”按照 Coglianese 教授和 Lazer 教授在一篇广被引用的文章中的分法,[26]监管规则可以分为三类:“以技术为基础的规制”、“以绩效为基础的规制”、“以管理为基础的规制”。在“以技术为基础的规制”中,监管规则明确要求被监管对象采用特定的技术或指定了规定动作;在“以绩效为基础的规制”中,监管者明确要求被监管对象取得一定的结果或者避免某些后果,至于被监管对象如何取得这样的结果,监管者不做任何规定;在“以管理为基础的规制”中,监管者既不规定具体的技术、动作、措施,也不规定结果、绩效,而是要求被监管对象以某一目标为导向,履行一定的内部流程,并落实流程中制定的内部计划和内部规则等。我国现有的安全保护义务主要是一项项具体的安全措施,因此可以被归类于“以技术为基础的规制”。

(2)缺乏动态考量。首先,信息安全等级保护制度中对系统的定级不考虑外部风险变化。一般来说,有效地管理信息系统面临的风险是保障网络安全题中之义。[27] 风险管理的第一步是风险评估,主要内容是评估侵害频率和侵害程度两个方面。[28] 因此,在评估中有三个因素不可或缺:威胁(谁发动攻击)、弱点(攻击如何开展)、影响(攻击能造成的后果)。[29] 通过威胁和弱点,能够估算出系统遭受侵害的频率。但在我国的信息安全等级保护制度中,系统定级的依据仅仅是“侵害的客体和对客体造成侵害的程度”,缺乏侵害发生的频率这一项,而恰恰是对侵害频率的预估,能让系统的安全保障体系锚定系统所处环境的各种变化。因此,仅仅关注侵害后果,忽略了动态变化的侵害频率,使系统安全保护工作失去了“相时而动”的机会。

---

〔26〕 Cary Coglianese and David Lazer, 2003, Management-Based Regulation: Prescribing Private Management, *Law and Society Review* 37 (4): 691 – 730. 在本文中,“具体的措施性规定”与“以技术为基础的规制”具有相同含义。

〔27〕 Eric A. Fischer, Cybersecurity Issues and Challenges: In Brief, Congressional Research Service, April 29, 2015. p. 2. http://digital. library. unt. edu/ark:/67531/metadc501605/,最后访问日期:2016 年 7 月 18 日。

〔28〕 Robert F. Weber, An Alternative Story of the Law and Regulation of Risk Management, *The University of Pennsylvania Journal of Business Law*, Vol. 15, No. 4 pp. 1005 – 1074, 2013.

〔29〕 Eric A. Fischer, Cybersecurity Issues and Challenges: In Brief, Congressional Research Service, April 29, 2015. p. 2 http://digital. library. unt. edu/ark:/67531/metadc501605/,最后访问日期:2016 年 7 月 18 日。

其次,等级保护仅仅要求“静态式的合规”。从完成测评后到下一次测评开始前的这段时间中,网络运营者要做的只是保证与分级相配套的各项安全措施持续运行即可,不用考虑网络安全攻防技术进步,只要不少做但也不用多做(如果定级不变的话,更是长年实施相同的安全措施),即算合规。至于实际防护效果如何,却不是评判是否履行安全保护义务的主要考量。例如,耗费巨资的中国铁路客户服务中心网站(简称 12306 网站)定为等级保护四级,但还是发生了被黑客拖库的事件。[30]

(3)关注安全底线。《信息系统安全等级保护基本要求》被定位为系统安全保护、等级测评的一个基本“标尺”,同样级别的系统使用统一的“标尺”来衡量。各级系统安全技术和安全管理要求是实现安全保护能力的一个达标线;每个级别的信息系统按照基本要求进行保护后,信息系统具有相应等级的安全保护能力,达到一种基本的安全状态。[31]因此有评论认为,等级保护主要关注通用的一些安全要求,并没有触及到用户安全需求的实质。[32]

二 现有的制度设计不足以保障实质性的网络安全

无论是现行制度,还是《网络安全法(草案)》,规定网络运营者的安全保护义务的基本路数是:由政府主导至上而下施加义务,并通过国家、行业标准规定非常具体的措施性要求作为义务的主要内容,然后通过行政处罚等手段强制性要求管理对象合规。但仅关注底线的、静态的、措施性的安全保护义务的基本逻辑,在现实中足以实现保障网络安全的目标吗?

(一)措施性的规定很可能造成“合规而非实质性安全”的情况

2015 年 7 月初,知名美国网络安全厂商 Triumfant Security 的首席执行官约翰·普里斯科发表了一篇名为《网络安全行业的百亿美元骗局》的文章,[33]在业内引起不小的震动。在他看来,虽然全球网络安全市场将在未来四年内从 750 亿美元增长到 1557.4 亿美元,但从 2009 年开始网络安全事故每年都增长 66%。“网络安全产业就是一场‘骗局’,厂商们都知道自己的产品根本解决不了问题,但依然卖得不亦乐乎。”

为什么产品解决不了问题?原因是经典的反病毒程序能发挥作用的前提是类似的攻击以前曾被安全厂商经历过,这些软件必须“依赖于对过去攻击的知识储备”。换句话说,这些产品的工作原理是把遇到的代码与其积累的攻击样本库进行比对,特征符合一致才能判断为恶意代码。而“现代网络罪犯更加复杂和高端”且有雄厚的资金支持。因此,样本库必然会过时,注定囊括不了所有情况。而且从发现威胁、分析威胁、形成具体的或

〔30〕 张伟丽:《信息安全等级保护现状浅析》,《信息安全与技术》2014 年第 9 期,第 12 页。

〔31〕 马力、毕马宁、任卫红:《国家信息安全等级保护政策中等级概念之间相互关系的分析》,《信息网络安全》2010 年第 11 期,第 5 页。

〔32〕 “2013 年信息安全产业将步入转折期”,http://www.ihep.cas.cn/zdsys/ihepsec/sec_ihep4/201301/t20130108_3747980.html,最后访问日期:2016 年 7 月 13 日。

〔33〕 John Prisco, “The cybersecurity industry's billion dollar scam”, July 3, 2015, http://thenextweb.com/insider/2015/07/02/the-cybersecurity-industrys-billion-dollar-scam/,最后访问日期:2016 年 7 月 13 日。

通用的特征规则,往往需要一定的时间。面对这样的局面,“保障网络安全,需要在不查询已知样本库的情况下分辨出正在遭遇的状况”。[34]

诚然,普里斯科把整个网络安全行业归为骗局的观点过于极端,[35]基于样本的传统杀毒软件也还将在系统防护中承担一定的角色,[36]但可以肯定的是,传统杀毒软件发挥的作用会越来越有限,正如美国著名智库兰德公司在报告中指出的,样本库实际上给黑客指明了攻击的方向,只要写出的攻击程序在样本库中没有被收录,那系统防护措施就如同马其顿防线一样,可以被轻易地规避。[37]

当下,杀毒软件正在经历一个范式上的变化:新一代的杀毒软件不再仅仅依赖病毒样本,转而重点监控、分析计算机上正在运行的各项进程、正在发生的各种变化和链接,目的是捕捉、识别出行为上的异常,以此作为系统遭受攻击、入侵的迹象。[38] 用形象的比喻来说,正常的员工进入工作场所后一般会径直进入自己的办公室,但坏人即便能通过伪造合法身份成功进入工作场所,因为不熟悉环境,往往会窥探每个房间寻找有价值的目标。新一代的杀毒软件能记录下系统内部所有的行为,并与正常的行为比对,以此发现不正常状况的端倪。

新一代杀毒软件更能适应目前瞬息万变的安全形势已经成为网络安全业界的共识。事实上,美国 2013 年国防预算法案(H. R. 4310)就已明确要求国防部下一代主机网络安全系统所采用的技术必须能够“应对新的或快速变形的威胁”。[39] 针对该法案的这项要求,美众议院军事委员会提出了如下建议:国防部应该获得“检测和防护尚未研究发现识别特征的网络威胁的能力”。[40]

但回到《网络安全法(草案)》和我国现行体制中,我们会发现没有相关的条款要求或者鼓励网络运营者使用新一代的杀毒软件。例如,《信息系统安全等级保护基本要求》发布于 2008 年,新一代杀毒软件还未成形,自然只能规定“应安装防恶意代码软件,并及时更新防恶意代码软件版本和恶意代码库”;再如,《网络安全法(草案)》第十七条第(二)款规定,“采取防范计算机病毒和网络攻击、网络入侵等危害网络安全行为的技术措施”。

---

〔34〕 John Prisco, “The cybersecurity industry's billion dollar scam”, July 3, 2015, http://thenextweb.com/insider/2015/07/02/the-cybersecurity-industrys-billion-dollar-scam/,最后访问日期:2016 年 7 月 13 日。

〔35〕 Jeff Clark, “Is Cybersecurity a Scam?”, July 7, 2015, http://www.datacenterjournal.com/cybersecurity-scam/,最后访问日期:2016 年 7 月 13 日。

〔36〕 Bob Violino, “Antivirus doesn't work. So why are you still using it?”, Apr 6, 2015, http://www.computerworld.com/article/2905871/antivirus-doesn-t-work-so-why-are-you-still-using-it.html,最后访问日期:2016 年 7 月 13 日。

〔37〕 Martin C. Libicki, Lillian Ablon, Tim Webb, The Defender's Dilemma: Charting a Course Toward Cybersecurity, 2015, RAND Corporation, pp. 27 – 28. http://www.rand.org/pubs/research_reports/RR1024.html,最后访问日期:2016 年 7 月 18 日。

〔38〕 Tim Greene, “Next-generation endpoint protection not as easy as it sounds”, Jul 20, 2015, http://www.networkworld.com/article/2949863/security/next-generation-endpoint-protection-not-as-easy-as-it-sounds.html,最后访问日期:2016 年 7 月 13 日。

〔39〕 See National Defense Authorization Act for Fiscal Year 2013, H. R. 4310, SEC. 932. Next-generation host-based cyber security system for the Department of Defense. https://www.govtrack.us/congress/bills/112/hr4310/text,最后访问日期:2016 年 7 月 13 日。

〔40〕 See Report of the Committee on Armed Services, House of Representatives, on H. R. 4310, Detection of Non-Signature Based Cyber Threats, http://www.gpo.gov/fdsys/pkg/CRPT-112hrpt479/html/CRPT-112hrpt479.htm,最后访问日期:2016 年 7 月 13 日。

不难想象,投机取巧的网络运营者可以选用花费较低的传统杀毒软件,而同样声称自己已经完整地履行了安全保护义务。实际上这不是简单的臆想,外国学者已经发出“反病毒软件依然被部署的原因不过是要满足法律和合规的要求而已”的抱怨。[41]

因此,措施性的规定很可能造成管理对象(在本文中也就是网络运营者)仅仅止步于合规,而缺乏动力去采用国家标准和行业标准要求之外的安全措施,哪怕是这些安全措施确实能提高安全水平。

(二)业态变化挑战过去行之有效的防护思维

守卫住系统边界曾被计算机和网络安全防护奉为圭臬。[42] 在组织和机构的信息入口和出口非常单一的情况下,包括防火墙、入侵检测和防御系统在内的守护边界的防御行之有效。传统安全遵循的防护思路是将防火墙和入侵防御系统放置在网络的外围,用以创建不可信外部与可信内部之间的边界。位于可信内部的各系统可以畅通无阻地处理其合法业务,而潜在的入侵者则都被封锁在防火墙之外。

然而,随着移动互联网、万物互联(Internet of Things)的不断推进,以及大量可联网智能设备的涌现,系统边界正在不断扩大。对攻击者来说,边界的扩大意味着“攻击面”在迅速扩大,可攻击的目标在增多,造成信息安全防御链条越来越长,信息安全防御面临越来越大的压力。[43]

与此同时,信息网络系统的边界正在模糊或弱化。例如,员工在工作场所用自有的设备(如 PAD、智能手机等)接入公司网络越来越成为普遍的行为,而这些设备往往也在其他场合使用,这就给黑客提供了一个便利的通往公司内网的通道:黑客只需在其他场合向员工自有设备植入木马或病毒,一旦这些设备接入内网,也就相当于木马和病毒绕过了严密的防火墙。[44]

再以前文提到的美著名零售公司 Target 超过 1 亿顾客信息泄露事件为例,黑客并没有直接攻击 Target 的支付网络,而是研究 Target 的供应链各个环节,选定了 Target 的一家第三方供应商为跳板,使用钓鱼邮件窃取了该供应商的用户凭证,从而获得进入 Target 网络系统的权限。随后,黑客通过在 POS 系统中植入软件,感染了所有刷卡机,截取了刷卡机上的信用卡信息,并最终成功入侵数据中心,窃走了所有的用户信息。[45] 在现实中,第三方供应商、业务合作伙伴和客户都经常需要访问企业或机构的网络,Target 错就错在盲目信任了供应链中环节,将其纳入自己系统边界的内部,仅仅要求他们提供基本的用户名和密码进行身份验证即可访问 Target 的内部网络。

边界保护变得越来越难,一旦内网边界被突破,内部网络实际上跟互联网一样危险。因此,2015 年 5 月,谷歌宣布不再将自身的企业应用置于防火墙等安全设备的保护之下,

〔41〕 Bob Violino, “Antivirus doesn’t work. So why are you still using it?”, Apr 6, 2015, http://www.computerworld.com/article/2905871/antivirus-doesn-t-work-so-why-are-you-still-using-it.html,最后访问日期:2016 年 7 月 13 日。

〔42〕 Joseph Migga Kizza, *Guide to Computer Network Security*, Springer-Verlag London, 3rd. 2015, v.

〔43〕 程彦博:《2015 信息安全趋势和任务》,《中国计算机报》2015 年 1 月 19 日第 6 版。

〔44〕 Zeus Kerravala, “Why cybersecurity needs to be adaptive”, May 28, 2015, http://www.networkworld.com/article/2927531/cisco-subnet/why-cybersecurity-needs-to-be-adaptive.html,最后访问日期:2016 年 7 月 13 日。

〔45〕 Congressional Research Service, “The Target and Other Financial Data Breaches: Frequently Asked Questions”, February 4, 2015, https://www.fas.org/sgp/crs/misc/R43496.pdf,最后访问日期:2016 年 7 月 13 日。

也就是说,谷歌将不再区分公司内网和外网。边界在扩大的同时也在弱化,直接挑战了在我国信息安全等级保护体制和现有国家、行业标准中占核心位置的“分区、分级、分域”防护策略和相应配套的各类措施性规定。[46]

(三)不断升级的攻防博弈将静态的标准远远拉下

说到底,信息安全就是攻方和守方之间较量达到的均衡状态。争锋相对,两方自然斗智斗勇,博弈不断升级。但近年来,似乎发动攻击的一方逐渐占了上风,不少企业的首席信息安全官都持有这样的观点。[47] 用其中一位的话说,“攻击者真的是太聪明、太有耐心、太贪婪”,[48]甚至于雇佣更多的安全人员并没有给企业带来更多的安全感。[49] 在2015年全球网络安全行业最权威的RSA大会中,有200位安全界专业主管接受问卷调查,超过75%的受访人认为主要原因是“进攻方式的演变太快了,根本无法跟上”。[50] 在此举两个例子具体说明:

物理隔离(Air-gapped):信息、网络系统没有直接接入互联网,也不与其它接入互联网的设备相连。采用物理隔离的系统好比是与世隔绝的孤岛,自然入侵者无法通过因特网侵入。目前,物理隔离被认为是保护机密数据最为有效的方法,为政府内网、支付系统、军事、关键基础设施的工业控制系统等所采用。目前我国国家标准和行业标准也要求高等级的系统采用物理隔离的方式。然而,道高一尺,魔高一丈,到目前为止,黑客们至少已经研究出八种方式跨越物理上的障碍,可以“隔空”入侵系统。

高级持续性威胁(Advance Persistent Threat,简称APT):采用定制化的手段、利用社会工程学,有计划、有组织地持续窥探目标网络弱点,长期潜伏并窃取核心机密数据。[51] 目前国内外安全业界公认,APT攻击普遍具备国家或有组织背景,针对的目标都是具有重大信息资产,如国家军事、情报、战略部门和金融、能源等影响国计民生的行业,已经成为网络安全最大的威胁。[52]例如360公司2015年发布报告,揭露从2012年4月起至今,某境外黑客组织对中国政府、科研院所、海事机构、海域建设、航运企业等相关重要领域展开了有组织、有计划、有针对性的长时间不间断攻击。[53] 要防御APT攻击非常困难,原因是

---

〔46〕 “新计算时代 等级保护建设面临新挑战”,http://security.zdnet.com.cn/security_zone/2013/0702/2166516.shtml,最后访问日期:2016年7月13日。另见江雪、何晓霞:《云计算时代等级保护面临的挑战》,《计算机应用与软件》2014年第3期,第293页。

〔47〕 Martin C. Libicki, Lillian Ablon, Tim Webb, The Defender's Dilemma: Charting a Course Toward Cybersecurity, 2015, RAND Corporation, p. 13. http://www.rand.org/pubs/research_reports/RR1024.html,最后访问日期:2016年7月18日。

〔48〕 Martin C. Libicki, Lillian Ablon, Tim Webb, The Defender's Dilemma: Charting a Course Toward Cybersecurity, 2015, RAND Corporation, p. 13. http://www.rand.org/pubs/research_reports/RR1024.html,最后访问日期:2016年7月18日。

〔49〕 Lee Munson, “Organisations Say Attacks Are Evolving Too Quickly, Recruitment Tricky”, July 22, 2015, http://bh-consulting.ie/securitywatch/?p=2702,最后访问日期:2016年7月13日。

〔50〕 Lieberman Software, http://www.liebsoft.com/2015-information-security-survey/,最后访问日期:2016年7月13日。

〔51〕 趋势科技:《演化的APT治理战略—— 使您不再因为APT攻击而感到恐惧》白皮书,2015年6月,第3页,http://www.trendmicro.com.cn/cloud-content/cn/pdfs/20150624.pdf,最后访问日期:2016年7月17日。

〔52〕 胡惠君:《网络安全审查制度要高度重视高级持续性威胁(APT)》,《中国信息安全》2015年3期,第10页。

〔53〕 天眼实验室,“OceanLotus(海莲花)APT报告摘要”,http://blogs.360.cn/blog/oceanlotus-apt/,最后访问日期:2016年7月13日。

APT 攻击渠道的多元化导致很难使用技术手段建立一张防护网来防止攻击;APT 攻击空间也不确定,任何一个阶段、任何一个网络都有可能成为攻击的目标,包括边缘性的、非核心的节点。[54]

从这两个例子,可以看到信息安全等级保护体制和现有静止的国家、行业标准已无法跟上攻防博弈的节奏,甚至在某种意义上还有可能成为安全的"负担",例如 APT 攻击者完全可以按照标准来了解某一系统布防的各个环节,并借着"这个地图"绕道而行。

(四)标准不可避免落后于现实需要

标准以科学、技术和实践经验的综合成果为基础,因此标准往往需要等待实践经过一定时间的发展和积累,然后"向后看",再总结、扬弃。从本质上说,标准必然滞后于实践。例如大家耳熟能详的智能设备、大数据、物联网、智慧城市等热点领域的信息安全标准尚未成形,但实践却早已跑到前面。以智能汽车为例,不久前美国两位安全研究员展示了如何利用"零日漏洞"远程控制一辆切诺基吉普车的通讯服务系统。一开始,两位研究员只是远程打开了汽车的空调、广播、挡风玻璃刮水器,而后他们开始直接控制汽车的驾驶速度,并最终让汽车停在了一个斜坡上。这次演示证明了黑客完全有可能远程关掉引擎,踩下刹车,甚至还能完全控制整辆车。据估计,目前市面上大约有 47 万辆汽车存在此漏洞。[55] 克莱斯勒甚至为此召回 140 万辆汽车。[56] 而在美国,针对智能汽车安全和隐私标准的全国性立法还仅仅处于提案阶段。[57]

2015 年 7 月初,中国国务院印发了《关于积极推进"互联网 +"行动的指导意见》,提出了 11 个具体行动,包括"互联网 +"创业创新、协同制造、现代农业、智慧能源、普惠金融、益民服务、高效物流、电子商务、便捷交通、绿色生态、人工智能。一方面,"互联网 +"在加速提升产业发展水平,增强各行业创新能力时,也引入了对这些领域来说十分陌生的互联网安全风险。另一方面,每个行业都有其自身的业务特征,在与互联网结合的过程中,还会产生各不相同的新技术、新业态,带来截然不同的信息安全问题,例如"互联网 + 金融"要解决的身份认证、纠纷解决等安全问题,显然与"互联网 + 制造业"中生产、调配等环节涉及的安全问题有很大不同。[58]

目前,"互联网 +"刚刚起步,可以预见除了国家标准外,各个行业很可能都需要自己的安全标准,而且国家标准和每个行业安全标准的制定和颁布也可能需要经过较长的时间。那么在标准发布之前,是不是说网络运营者就不需要承担安全保护义务了?再进一步,瞬息万变的网络安全形势,层出不穷的未知漏洞、威胁、攻击方式,使已有的国家标准、行业标准面临必须迅速更新、时时更新的压力,甚至还可能出现制定出的安全标准还未发

〔54〕 鹿宁宁:《APT:攻击容易 防御不易》,《网络世界》2014 年 4 月 21 日第 32 版。

〔55〕 Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway—With Me in It", July 21, 2015, http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/,最后访问日期:2016 年 7 月 13 日。

〔56〕 BBC, "Fiat Chrysler recalls 1.4 million cars after Jeep hack", 24 July 2015.

〔57〕 Alexander Howard, "Senate Bill Aims To Lock Hackers Out Of Connected Cars", The Huffington Post, July 21 2015, http://www.huffingtonpost.com/entry/spy-act-car-hackers-senators-security_55ae4e72e4b0a9b94852748b,最后访问日期:2016 年 7 月 13 日。

〔58〕 吕本富、张崇:《"互联网 +"环境下信息安全的挑战与机遇》,《中国信息安全》2015 年第 6 期,第 13 页。

布就已经过时的局面。[59]

（五）总结：愈发重要的“其他必要措施”

在这个变化的时代，由现有的主要关注安全底线、以措施性内容为主、静态的信息安全等级保护的国家和行业标准来界定安全保护义务（也就是“责”的内容），已经很难达到保障信息系统和网络实质性安全的目标。但是不是应就此抛弃这些国家和行业标准？对此，笔者坚决反对。“在对抗性不强的非国家安全领域，合规性并不是太大的问题，金字塔形的资质需求也许是有效的。”[60] 甚至于在笔者看来，强制性的信息安全等级保护国家、行业标准是十分必要的，毕竟通过合规，各系统和网络具备了基本的安全能力。

应该竭力避免的局面是，“各种意义上的‘合规性’检验取代了实质性的能力建设”，毕竟“挂在墙上的资质证书完全无法应对真刀真枪的战略威胁。”[61] 事实上，《信息系统安全等级保护基本要求》也将自身定位为“出发点”，建议网络运营者“调整和补充基本安全要求，从而实现信息系统在满足等级保护基本要求基础上，又具有自身特点的保护”。

但应该如何使网络运营者不止步于“国家标准、行业标准的强制性要求”？目前的《网络安全法（草案）》仅仅规定了兜底条款——“其他必要措施”。换句话说，《网络安全法（草案）》希望通过“其他必要措施”来确保广大网络运营者在无标准可依或标准不足以提供实质性安全时，也不能推卸保护义务。

2015 年，RSA 大会的主题定为“改变：挑战当今的安全理念”。[62] 这次会议召开的背景是：“传统的安全防御手段显然早已落后于现实中网络技术发展的脚步，固有的安全理念无时无刻不在接受新威胁形势的挑战。”[63] 而会议透露出的核心信息即是，“在这个变化的时代，唯有用变化方能成功地应对变化”。

这么看来，未来保障网络安全的关键之关键，将是如何在实践中随着安全形势变化来确定“其他必要措施”的具体所指。但非常遗憾的是，目前《网络安全法（草案）》对此基本没有考虑。

三　美、欧对安全保护义务的立法逻辑

（一）“合理性”原则作为安全保护义务的主要评价标准

与我国的“必要措施”类似，美国主要的信息安全法律在相关规定上大都采用“合理

〔59〕 Kenneth L. Wainstein and Keith M. Gerver, “The Rockefeller letter and the cybersecurity debate”, Oct 12, 2012, http://www.cadwalader.com/resources/clients-friends-memos/the-rockefeller-letter-and-the-cybersecurity-debate，最后访问日期：2016 年 7 月 13 日。

〔60〕 沈逸，“网络安全法草案：为建设网络强国提供制度保障”，澎湃新闻，2015 年 7 月 16 日，http://m.thepaper.cn/newsDetail_forward_1353139，最后访问日期：2016 年 7 月 13 日。

〔61〕 沈逸，“网络安全法草案：为建设网络强国提供制度保障”，澎湃新闻，2015 年 7 月 16 日，http://m.thepaper.cn/newsDetail_forward_1353139，最后访问日期：2016 年 7 月 13 日。

〔62〕 “2015：Change：Challenge today’s security thinking”，http://www.rsaconference.com/about/themes，最后访问日期：2016 年 7 月 13 日。RSA 大会是全球最大规模的企业信息安全领域的会议，每年的 2 月下旬或 4 月下旬固定在旧金山举行，被誉为网络安全领域的“奥林匹克运动会”，2015 年的 RSA 大会热度较 2014 年有大幅提高，出席人数有三万之众，参展商逾 五百。RSA 已成为全球网络安全的风向标。

〔63〕 鹿宁宁：《唯一不变的就是变化——RSA 2015 纵览》，《网络世界》2015 年 5 月 4 日第 8 版。

性”这个概念,例如健康保险携带和责任法案、金融业的格雷姆—里奇—比利雷法案、儿童在线隐私保护法案等,都使用了“合理的措施”、“合理的设计”、“可合理预见的”等概念。[64] 在欧洲,主要的网络安全立法草案采用了与“必要”、“合理”非常相似的“合适性”。

但与我国安全保护义务“以国家和行业标准为主、其他必要措施兜底”不同的是,美、欧将“合理性”、“合适性”这样的概念作为安全保护义务的主要评价标准。采取这样的立法模式,避免国家强制划定统一的安全模式,给各个企业和机构根据各自商业模式制定不同的网络安全策略足够的空间。[65] 其背后主要有以下几个方面理由:

首先是技术进步导致具体的措施性安全义务制定出来后就面临迅速过时、效率降低、成本增高等问题。立法者为避免需要经常性地修订安全义务的规定,偏向采用“合理”、“合适”这类在不同时期可以有不同内涵的概念。[66]

其次是信息不对称。被监管对象具有对自身所处环境、所面临的风险、以及运营各个环节等方面的一手信息和知识,监管者如果强行施加统一的、具体的措施性的安全义务,很可能造成事倍功半甚至力道用错了地方的局面。[67]

最后是网络安全的监管部门面向的是社会各行业。不同行业之间高度异质,而且即使在同一行业内部,不同网络运营者由于规模、资源、存储信息种类等差异,也存在统一的具体性措施或标准适用程度不一的问题。[68]

由上可知,美、欧在立法时考虑到了通过关注安全底线、以措施性内容为主、静态的标准来界定安全保护义务可能导致的问题,所以主要采用“不确定的法律概念”实现规范性要求和现实之间的妥协,但并不是说美欧就完全抛弃标准,只不过标准更多的是一种开展安全保护工作的重要参考,特别是美国。

(二)通过“以管理为基础的规制”来界定“合理性”

“合理”、“合适”缺乏确定的含义,仅仅依靠这样的限定作为安全保护义务的评价标准未免过于单薄、草率。美、欧立法一个非常显著的特点即是通过“以管理为基础的规制”来进一步界定“合理性”。

“以管理为基础的规制”以监管对象内部的管理流程、模式为着力点,与“措施为基础的规制”的本质区别主要有两方面:一是规制发生作用的阶段不同,“以管理为基础的规制”在机构谋划、制定安全保护策略的阶段就入手,“以措施为基础的规制”则在安全保护策略的执行阶段生效。二是规制的具体要求不同,“以管理为基础的规制”作用于管理流程,要求组织内部的管理流程以某种目标为指导、符合一定的特征、履行一定的步骤,而

〔64〕 Peter Sloan, 2014, The Reasonable Information Security Program, 21 *Richmond Journal of Law and Technology* 2.

〔65〕 Denise E. Zheng and William A. Carter, 2015, The Evolution of Cybersecurity Requirements for the U. S. Financial Industry, Center for Strategic and International Studies, p. 6. https://www. csis. org/analysis/evolution-cybersecurity-requirements-us-financial-industry,最后访问日期:2016 年 7 月 18 日。

〔66〕 Denise E. Zheng and William A. Carter, 2015, The Evolution of Cybersecurity Requirements for the U. S. Financial Industry, Center for Strategic and International Studies, p. 27. https://www. csis. org/analysis/evolution-cybersecurity-requirements-us-financial-industry,最后访问日期:2016 年 7 月 18 日。

〔67〕 Derek E. Bambauer, 2014, Ghost in the network, *University of Pennsylvania Law Review*. 162(5), p. 1026

〔68〕 David Thaw, 2014, “The Efficacy of Cybersecurity Regulation,” *Georgia State University Law Review*: Vol. 30: Issue 2, p. 325.

“措施为基础的规制”主要规定落实安全保护策略时必须采用具体的安全措施和行为,两者层次不同。[69]

适用于网络安全领域,“以管理为基础的规制”,就是明确要求各企业机构对网络安全策略量体裁衣,并对内部决策、规划流程提出规范性要求。

1. 企业、机构层面的“以管理为基础的规制”

加利福尼亚州是硅谷所在地,因此在网络安全和数据保护方面的立法走在美国各州的前面。[70] 2015 年 6 月,加州众议院通过了旨在修订该州的《1977 年信息实践法》的第 83 号众议院法案。《1977 年信息实践法》规定,拥有、留存个人信息的商业机构,应当落实和保持“合理的安全程序和做法”,这些程序和做法“须与信息的种类相称”,且能够“保护个人信息免于未经授权的访问、使用、修改和公布”。

第 83 号法案进一步定义了“合理的安全程序和做法”的提法,要求企业实现的最低安全水平“不应低于任何一家合理审慎的商业机构会提供的安全水平”。具体来说,企业应做到以下四个方面:a)辨别出“可合理预期到的内部和外部风险”;b)建立、落实、保持“合理设计的”个人信息安全保护策略;c)定期评估保护措施是否足以应对“可合理预期到的内部和外部风险”,并根据评估结果调整保护措施;d)在商业运作和模式产生实质性变化,对个人信息安全或隐私造成实质性影响的情况下,对保护措施进行评估并调整。[71] 第 83 号法案规定的四个方面,构成了一个企业或机构内部风险管理流程的闭环:从风险评估,到制定保护策略,到定期评估风险变化并相应调整保护策略。

实际上,不仅是州一级的法律,联邦一级的主要信息安全立法也采用了“以管理为基础的规制”。Peter Sloan 教授综合分析了美国主要信息安全立法中对“合理性”的规定,归纳出 6 点核心要求:a)组织应准确辨识自身所拥有的、处理的、代管的、控制的信息类型;b)组织应评估在保护信息安全时可预见的威胁、弱点,以及风险;c)组织应建立应对上述威胁、弱点、风险合理的策略,以及行政、物理、技术上的措施;d)组织应处理在与第三方的关系中对信息安全可能造成的影响;e)组织应当在数据泄露发生后立即采取补救措施;f)组织应经常评估、更新信息安全保护策略和措施。[72]

不难看出,美国法律在评价某一组织是否履行了安全保护义务时,其实主要是在审视其内部的网络安全风险管理流程是否合理。

2. 国家网络安全层面的“以管理为基础的规制”

目前,美国网络安全领域的专门立法主要围绕两个方面展开:一是如何鼓励政府和网

---

〔69〕 Cary Coglianese and David Lazer, 2003, Management-Based Regulation: Prescribing Private Management, *Law and Society Review* 37(4): 691 - 730

〔70〕 Doneld G. Shelkey and Christopher C. Archer, June 26, 2015, “California Law to Watch: A New Standard for Data Security Compliance”, *The National Law Review*, http://www. natlawreview. com/article/california-law-to-watch-new-standard-data-security-compliance,最后访问日期:2016 年 7 月 13 日。

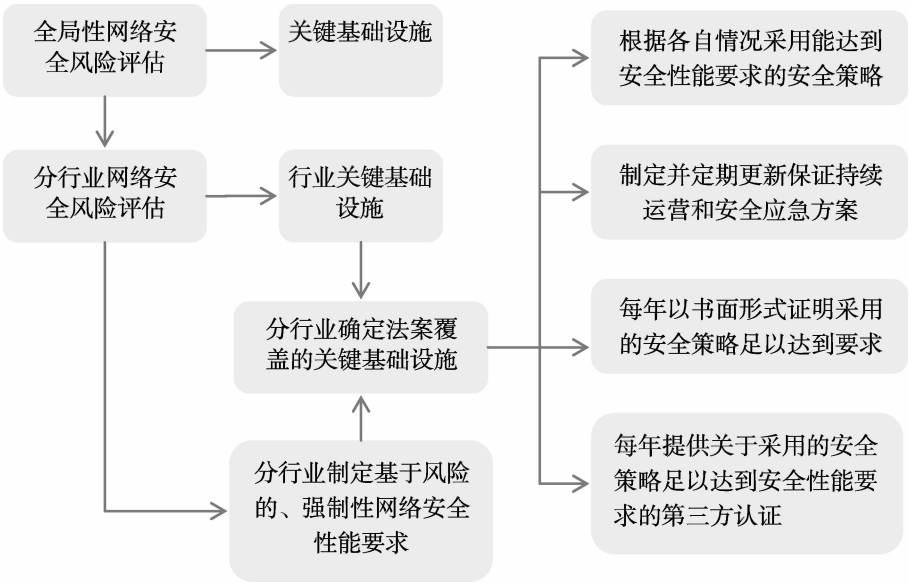
〔71〕 Doneld G. Shelkey and Christopher C. Archer, June 26, 2015, “California Law to Watch: A New Standard for Data Security Compliance”, The National Law Review, http://www. natlawreview. com/article/california-law-to-watch-new-standard-data-security-compliance,最后访问日期:2016 年 7 月 13 日。

〔72〕 Peter Sloan, 2014, The Reasonable Information Security Program, 21 *Richmond Journal of Law and Technology* 2.

络运营者之间,以及网络运营者之间更大程度共享网络威胁信息,二是数据泄露之后,网络运营者如何向政府职能部门、社会、以及受影响的个人报告、公布、提示。[73] 实际上,自2002 年通过《联邦信息安全管理法》以来,美国没有通过任何重要的综合性网络安全立法,[74] 真正意义上的综合性立法尝试只有《2012 年网络安全法案》。[75]

按照《2012 年网络安全法案》的制度设计(见图四),国土安全部首先在全美范围内关键基础设施开展全局性的网络安全风险评估,以判定哪一行业面临最严峻的网络安全风险;根据行业风险排名,分行业开展网络安全风险评估。分行业的网络安全评估结果非常重要:一是用来确定行业中哪些关键基础设施需要受《2012 年网络安全法案》的管辖,二是用来确定行业中受管辖的关键基础设施需要达到的、强制性的网络安全性能要求。之后,国土安全部将会制定规则,要求各行业受管辖的关键基础设施根据分行业的风险评估以及性能要求,根据各自情况制定、执行网络安全策略。每年,关键基础设施的运营者要以书面形式提交证明其安全策略足以达到强制性性能要求的报告,并需要提供第三方对此的认证。

图四:美国《2012 年网络安全法案》版本[76]



可见,《2012 年网络安全法案》从两个层次入手,先是规定了国土安全部开展国家网络安全工作的具体模式和流程:以风险评估为指导,全局性和分行业先后展开;根据风险

〔73〕 Mark A. Hofmann, Federal cyber security legislation possible in 2015 http://www. businessinsurance. com/article/20150517/NEWS06/305249993, 最后访问日期:2016 年 6 月 1 日。

〔74〕 青砚:《斯诺登阴影下的美国网络安全立法》,《中国经济周刊》2015 年第 6 期。

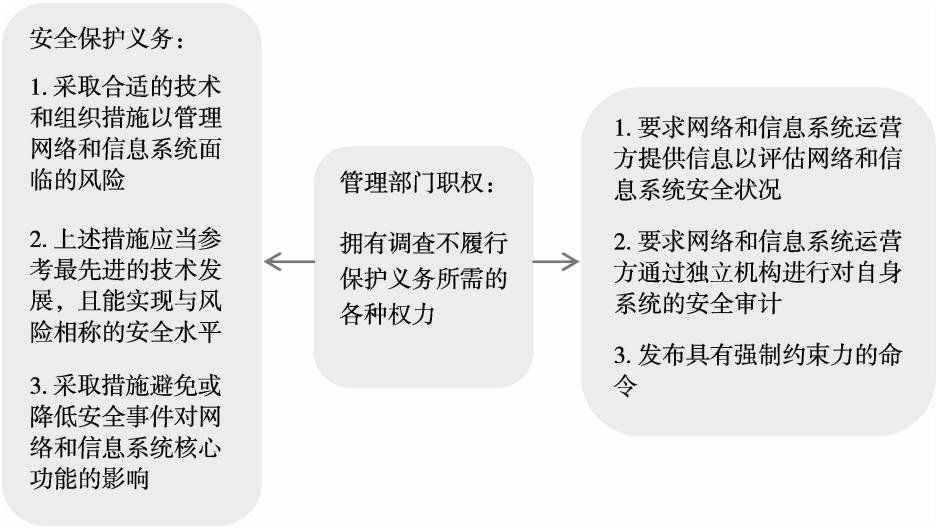
〔75〕 相关背景情况,见刘金瑞:《美国网络安全立法近期进展及对我国的启示》,《暨南学报》2014 年第 2 期。但《2012 年网络安全法案》(S2105)及其修改版本《2012 年网络安全法案》(S3414)均未成为法律。

〔76〕 笔者根据法案内容总结绘制。法案文本见 https://www. congress. gov/bill/112th-congress/senate-bill/2105,最后访问日期:2016 年 7 月 13 日。

评估确定规制对象和规制要求。随后,规制对象根据行业风险评估和规制要求,自行制定安全策略,并定期评估。最后,规制对象需要引入第三方来对其提出的安全策略给予背书。无疑,这是典型的“以管理为基础的规制”。

目前,欧盟层面关于网络安全方面的唯一立法——网络与信息安全指令——于 2015 年 12 月正式通过,并于 2016 年 7 月生效。[77] 按照网络与信息安全指令的制度设计(见图五),[78]监管对象需要评估网络和信息系统面临的安全风险,并采取“合适的”技术和组织措施应对风险。可见,网络与信息安全指令也主要从监管对象内部的安全风险管理流程切入并提出要求,以此作为监管对象安全保护义务的主要内容。

图五:欧盟网络信息安全指令



总结起来,就网络运营者的安全保护义务而言,美、欧在法律层面没有规定落实安全保护策略时应具体采用的技术或措施,而是要求网络运营者在设计安全保护策略时应遵循一定的原则和步骤,且都把风险管理作为设计安全保护策略的基本框架。

四 网络安全法为什么宜采用“以管理为基础的规制”

在安全保护义务方面,我国和美欧在思路上的区别可以用这么一个例子说明白:我国主要强调基础科目训练,不论是从事足篮排还是其他项目的运动员(类比于各个行业),只要是同一级别(例如市级、省级、国家级,类比于等保定级),都必须通过统一的、固定的科目测试(即保障安全底线、静态、措施性的安全保护义务),对这些基础科目之外的内容则考虑不多(即“其他必要措施”)。

〔77〕 Network and information security: breakthrough in talks with EP, JUNE 29 2015, http://www.consilium.europa.eu/en/press/press-releases/2015/06/29-network-information-security/,最后访问日期:2016 年 7 月 13 日。

〔78〕 笔者根据指令内容总结绘制。指令文本见 http://eur-lex.europa.eu/procedure/EN/202368,最后访问日期:2016 年 7 月 13 日。

美欧则要求运动员评估所处项目的特点和竞争情况(即分行业风险评估),自行提出符合自身条件的训练计划和希望达到的竞技目标(即各自制定安全策略),必要的情况下要求运动员将训练计划交给第三方评估、背书。运动员还得根据各自项目的变化调整自己的训练项目。

从直观感觉来说,大部分读者应该会更倾向于美欧的思路,毕竟美欧的做法更加有针对性,也更加经济。接下来,笔者将运用规制理论说明为什么网络安全领域适宜采用"以管理为基础的规制"。

首先,"以管理为基础的规制"直接作用于组织内部。常规的监管思路把组织当成一个分析单位,组织内部的架构、文化、决策流程等是"黑盒子",监管者不用考虑也不应该过问;监管者要么对组织的具体行为做出规定(做什么、不做什么),要么对组织的绩效做出规定(取得一定的成效或避免一定的结果)。而"以管理为基础的规制"则深入组织内部,把黑盒子打开,直接对组织的内部管理流程做出规定。其背后的理由是,组织在日常运营时面临着来自诸如消费者、供销商、同行、金融合作机构等各方面的压力,监管的压力只是其中之一。组织的行为,其实是内外各方面压力作用于组织内部的管理和决策的产物。换句话说,监管者要与其他方面的力量相互竞争,争取最大程度影响组织决策层,才能取得监管效果。与其这样,监管者还不如借助公权力的强制性,直接塑造组织的内部管理和决策;这样,组织面对的其他方面力量就只能在监管者提前设定的游戏规则里运作。[79] 因此,"以管理为基础的规制"应该能有效地解决网络安全领域长久以来的老大难问题——如何改变广大网络运营者的思维定式,从把安全当成一个额外的负担、一个"能省则省"的项目,转而真正地、发自内心地重视安全保护工作。

其次,"以管理为基础的规制"特别适用于监管对象高度异质、监管绩效很难衡量的领域。[80] 在监管对象"高矮胖瘦"都有的情况下,监管要求很难做到整齐划一,强行划线不仅会造成水土不服,客观上还很可能鼓励监管对象"上有政策、下有对策"。监管对象情况迥异还会加剧监管者面临的信息不对称程度,监管者很难凭经验来估计企业的情况,而且监管对象可以轻易地选择性披露信息,玩捉迷藏的游戏。此时,给监管对象定绩效指标而不规定实现方式是一个好的选择。但如果碰到监管绩效很难直观衡量的领域,"以绩效为基础的规制"就有可能失灵。为克服上述困难,以管理为基础的规制"将决策的责任赋予拥有大多数风险信息和潜在控制方法的企业,因此,企业自律行为将比政府施加监管标准成本更低也更有效率。通过允许企业做出自己的决定,管理者和雇主更有可能认为自己组织的规则更合理,上述规则能够比政府强加的标准更好地得到遵守。"[81]

---

〔79〕 Cary Coglianese and Jennifer Nash, 2015, "Using Public Law to Shape Private Organizations.", edited by Austin Sarat and Patricia Ewick, *The Handbook of Law and Society*, Blackwell Publishing, Chapter 11. pp. 168 – 182. http://onlinelibrary.wiley.com/book/10.1002/9781118701430,最后访问日期:2016 年 7 月 18 日。

〔80〕 Cary Coglianese and David Lazer, 2003, Management-Based Regulation: Prescribing Private Management, *Law and Society Review* 37 (4): 691 – 730.

〔81〕 Cary Coglianese and David Lazer, 2003, Management-Based Regulation: Prescribing Private Management, *Law and Society Review* 37 (4): 695 – 696.

网络安全正好符合监管对象高度异质、监管绩效很难衡量这两个特征。[82] 网络安全的本质是保证业务的安全。[83] 安全保护方案需建立于业务模式之上。而各行各业业务模式千差万别,同一行业上下游企业业务模式、规模、资源也非常不同,统一的、措施性的强制规定很难制定。[84] 网络安全措施取得的安全效果还很难量化。不少企业的首席信息安全官认为自己工作的难点之一,就是在于向企业管理层证明在安全上的花费具有成效,[85]因为安全是攻防之间的一种动态均衡状态,安全事故没有发生,并不表示安全措施就非常有效,很可能只是黑客没有盯上;同样,安全事故发生了,也不能说安全措施就一点用没有,有可能是不幸被有国家背景或资金雄厚的黑客组织发动了进攻。[86] 因此,没有哪个首席信息安全官敢拍着胸脯保证,一年以内网络安全事故能控制在几起以内。监管部门也很难做出类似的要求。

五 对我国网络运营者安全保护义务的立法建议

目前,全国人大法工委刚完成《网络安全法(草案)》二审,配套的实施细则也没有提上议程。因此,在文末笔者试着对我国网络运营者安全保护义务提出两套方案。

第一,如果说“关注安全底线的、静态的、具体措施性规定”为主的安全保护义务立法模式保持不变,那么《网络安全法(草案)》对“其他必要措施”就必须有所设计。对此,笔者建议鼓励行业组织、企业和安全服务厂商合作,根据形势和技术变化自主形成具有一定普遍性的安全标准和安全做法,作为国家、行业标准的补充和提升,并在实践中(监管和司法中)作为判断“其他必要措施”的重要参考。同时国家对自下而上形成的自愿性标准和做法给予某种形式的背书和法律责任减免等激励。

行业自主形成的经验和做法,更加灵活、更新起来更快、更贴近行业现状和运营现实,也有利于克服监管信息不对称的问题。此外,完全依靠国家主导制定的国家、行业标准,还将对安全行业造成不利影响。采用以措施性内容为主的国家标准、行业标准来规定网络运营方的安全保护义务,将会导致安全行业的发展被限定在国家标准、行业标准所设定的条条框框内。网络运营者没有动力去采用国家标准和行业标准之外的安全措施,将会造成市场对安全产品和服务的需求不足。需求一旦不足,就会造成安全企业创新动力不足,市场上安全产品和服务停滞不前。因此,现有的措施性、静态式的国家、行业标准,很可能会压缩安全行业的发展空间和活力。重视自下而上形成的自愿性标准和做法,并给

〔82〕 David Thaw, 2014, “The Efficacy of Cybersecurity Regulation,” *Georgia State University Law Review*: Vol. 30: Issue 2,

〔83〕 周雪:《安全的出发点不是“标准化”》,《信息安全与通信保密》2010 年第 9 期,第 12 页。

〔84〕 Martin C. Libicki, Lillian Ablon, Tim Webb, The Defender's Dilemma: Charting a Course Toward Cybersecurity, 2015, RAND Corporation, p. 10. http://www.rand.org/pubs/research_reports/RR1024.html,最后访问日期:2016 年 7 月 18 日。

〔85〕 Martin C. Libicki, Lillian Ablon, Tim Webb, The Defender's Dilemma: Charting a Course Toward Cybersecurity, 2015, RAND Corporation, p. 11. http://www.rand.org/pubs/research_reports/RR1024.html,最后访问日期:2016 年 7 月 18 日。

〔86〕 David Thaw, 2014, “The Efficacy of Cybersecurity Regulation,” *Georgia State University Law Review*: Vol. 30: Issue 2, p. 302.

与国家某种形式的背书,可以一定程度上缓和这种困境。

第二,更为彻底的改革模式是引入“以管理为基础的规制”,效仿美欧用风险管理的框架来塑造网络运营者认识、履行网络安全保护义务的方式。“以管理为基础的规制”改造组织内部的决策流程,起到治本的作用。同时风险管理要求评估危害发生的机率,能将动态的威胁和技术变化内化于决策流程中。在充分认识风险的基础上,“以管理为基础的规制”允许网络运营者灵活运用各种手段和措施有效应对风险。因此,笔者建议《网络安全法(草案)》第十四条和二十条将“风险评估、建立内部安全策略、执行策略、定期回顾改进”作为安全保护义务内容的主体框架,并以强制性国家、行业标准为辅。

“以管理为基础的规制”让网络运营者自己定计划、自己执行,怎么能保证充分的风险评估、设计的安全策略足够应对风险?对此,引入第三方认证是一个好的方式,美国《2012 年网络安全法案》就做出了这样的制度设计。另外一个值得借鉴的方式是明确将网络运营者的首席执行官或首席运营官定为网络安全负责人,并要求他们以个人名义、书面形式对其组织开展的风险评估和安全策略做出“认为其有效”的声明。[87] 一旦责任与个人挂钩,而且是企业高管而非安全技术主管,足以让组织认真对待。

第三,需要再次强调的是,上述两套方案均不是全盘否定以“关注安全底线的、静态的、具体措施性规定”为主要特征的信息安全等级保护国家和行业标准,毕竟要求网络和信息系统具备基本的安全能力还是具有重要的现实意义,也应该成为网络运营者安全保护义务的内容之一。但网络安全形势瞬息万变,网络运营者的安全保护义务应紧跟现实,具备动态性。

[**Abstract**] Like in most other countries, the majority of network operators in China belong to private sector. How to properly define their security obligations is one of the key questions of cyberspace security. In this regard, the current institutional designs and the Draft Cybersecurity Law of the PRC adopt an approach that emphasizes baseline security, are static, and mainly consist of concrete security measures. As the threat landscape of cybersecurity is changing rapidly, such an approach is not adequate to provide essential security to networks. The institutional design for the security obligation of network operators should focus on enabling network operators to attach sufficient importance to risk management in their internal management process.

(责任编辑:田 夫)

〔87〕 美国《1991 年联邦存款保险公司改进法案》即在银行风险控制方面做出了类似的规定。