

美国网络安全责任政策分析及启示

张烨阳, 李惟依, 韩 旻, 李 响, 夏春姊, 张 蕾
(中国科学技术信息研究所, 北京 100038)

摘要: 2023 年美国拜登政府发布了《国家网络安全战略》, 该战略以 2021 年发布的第 14028 号行政命令为基础, 对网络空间责任的分配方式做出了根本性的转变, 强调政府监管在市场中的作用。通过重塑市场格局, 将网络风险从最终用户转移到拥有数据和技术的各类企业实体。避免最终用户因专业人员、数据、技术等资源的匮乏而成为网络空间中最为薄弱的一环, 让最有能力确保网络安全的参与者肩负起相应责任, 以建设一个可防御、有弹性的数字生态系统。从战略的背景出发, 对战略平衡网络安全责任的举措进行了分析, 之后建立了网络安全边际收益曲线模型, 使用该模型对战略转移网络安全责任的政策方向合理性进行了判断, 对战略具体政策措施的有效性进行了分析, 最后提出了对中国网络安全空间责任分配政策的建议。

关键词: 网络安全责任; 网络安全战略; 数字生态系统; 网络保险

中图分类号: G323; TN915.08 **文献标识码:** A **DOI:** 10.3772/j.issn.1009-8623.2024.06.008

1 研究背景

近年来, 美国接连发生的 SolarWinds^[1]、Microsoft Exchange^[2]、Colonial Pipeline^[3] 等网络安全事件分别在政务信息安全、能源等关键领域对美国社会产生了重大影响, 使美国网络安全面临严重挑战。通过对以往经验的总结, 美国拜登政府认为仅靠市场力量不足以实现安全的数字生态环境。为了应对日益严峻的网络安全威胁, 美国在 2021 年第 14028 号《关于改善国家网络安全的行政命令》^[1] 和国家安全备忘录《改善关键基础设施控制系统的网络安全》^[4] 的基础之上制定了《国家网络安全战略》^[5] (以下简称“战略”)。战略由保卫关键基础设施、扰乱并瓦解具有威胁的网络行为、塑造市场力量增强网络安全和弹性、投资具有弹性的未来、锻造国际合作伙伴关系追求共同目标等 5 个战略支柱、27 个战略目标、65 项举措组成 (见表 1)。相比前几届美国

政府的国家网络安全战略, 该战略以建设一个可防御、有弹性的数字生态系统为目标, 对市场的激励方式、网络空间责任的分配方式做出了根本性的转变, 强调政府监管在市场中的作用, 通过重塑市场格局, 将网络风险从最终用户 (如个人、小型企业、州和地方政府以及基础设施运营商) 转移到拥有数据和技术的各类企业 (如技术公司、软件供应商、云服务提供商等)。避免最终用户因专业人员、数据、技术等资源的匮乏而成为网络空间中最为薄弱的一环, 让最有能力确保网络安全的参与者肩负起相应责任, 以建设一个可防御、有弹性的数字生态系统。为此, 战略建议制定相应法律, 让未采取合理预防措施保护其产品和服务的实体需担负责任。

在平衡网络安全责任方面, 各国近年来都有所探索。2024 年 3 月欧盟议会批准了新的产品责任指令, 这是 40 年以来首次对《产品责任指令》的修订^[6-7], 新修订的文件将软件、硬件纳入指令范围,

第一作者简介: 张烨阳 (1984—), 男, 硕士, 高级工程师, 主要研究方向为网络安全。

项目来源: 中信所重点工作项目“中信所统一数据底座建设与运营管理 (二期)” (ZD2024-06); 国家科技图书文献中心 2024 年专项任务“数据安全管理体系研究” (2024XM14)

收稿日期: 2024-04-16

表 1 美国国家网络安全战略中的战略支柱及部分目标、措施

战略支柱	部分战略目标	部分举措
保卫关键基础设施	制定网络安全要求以支持国家安全和公共安全	建立网络安全法规以保护关键基础设施
	扩大公私合作	加强部门风险管理机构（SRMA），使其能够主动响应行业关键基础设施所有者和运营商的需求
	在美国联邦政府中推广现代化网络防御技术	在联邦文职机构中继续推广零信任架构战略
扰乱并瓦解具有威胁的网络行为	整合美国联邦网络打击力量	美国司法部和其他联邦执法机构将整合私营企业、合作伙伴的力量打击网络犯罪活动
	加强公私合作以打击对手	美国联邦政府将组织美国 ICT 制造商和服务提供商（以下简称“私营部门”）打击对手
	打击网络犯罪，击败勒索软件	美国联邦政府将动用国家力量破坏勒索软件生态系统，并孤立为犯罪分子提供避风港的国家
塑造市场力量增强网络安全和弹性	让数据管理员承担责任	美国联邦政府将支持通过立法，对收集、使用、传输、维护个人数据施加有力、明确的限制
	推动安全物联网设备的发展	美国联邦政府将按照《物联网网络安全改进法案》改善物联网网络安全，并继续推进物联网安全标签计划
	转移不安全软件产品和服务的责任	美国联邦政府将与美国国会、私营部门一起制定法律，确立软件产品和服务的责任
	利用美国联邦政府采购加强问责	美国司法部将根据《虚假申报法》，使用民事网络倡议对未能履行网络安全义务的承包商提起诉讼
	探索美国联邦网络保险制度	美国联邦政府将评估联邦保险应对灾难性网络事件的必要性
投资具有弹性的未来	确保互联网关键性技术安全	美国联邦政府将与利益相关者合作，解决目前网络协议中的安全问题
	重振美国联邦网络安全研究与开发	继续推动美国联邦网络安全研究与发展战略，主动预防和降低下一代技术中的网络安全风险
	为后量子时代做好准备	加强对公共网络和系统的保护，使其可以抵御量子密码学的攻击
锻造国际合作伙伴关系追求共同目标	建立《互联网未来宣言》合作伙伴联盟以应对数字生态系统的威胁	美国将与盟国和伙伴国合作，为数字时代建设新的协作执法机制
	确保信息、通信和运营技术产品与服务的全球供应链安全	美国将与盟国和伙伴国合作，努力将信息通信领域供应链转移至国内或伙伴国家

将产品网络安全漏洞视为产品缺陷，更新了缺陷检验标准，扩大了消费者追偿范围，其政策最大的特点是采用了严格责任制度。2022年10月6日英国《产品安全和电信基础设施法案》获得批准^[8]，该法案要求联网设备制造商必须遵守相关规定，在提升设备预置默认密码强度、建立重要安全更新通知制度、建立安全漏洞报告制度等方面履行网络安全义务。忽视该网络安全义务的设备制造商将被处以最高

1 000 万英镑或其全球营业额 4% 的罚款（以较高者为准），罚款后若违规行为持续存在，则额外处以每天 2 万英镑的罚款。2023 年 11 月 22 日澳大利亚发布了《2023—2030 年网络安全战略》^[9]，旨在 2030 年前发展成为网络安全领域的世界领导者，该战略拟明确国家重要系统及关键基础设施中私营实体的网络安全义务，在软件设计中推广最佳安全实践。但战略并未明确私营实体忽视网络安全义务

所应承担的责任,在推广最佳安全实践方面也遵循自愿原则。与美国相比,英国、澳大利亚、欧盟国家及地区市场规模较小、大型信息与通信(ICT)企业数量较少,美国在此方面的政策对中国更具借鉴意义。美国作为世界信息产业的发源地和在 ICT 领域实力最为强大的国家,其网络安全政策的一举一动都颇受关注。这项极具变革性的战略将为美国未来的数字生态环境带来深刻的影响。本文从战略的背景出发,对战略平衡网络安全责任的举措进行了分析,之后根据网络安全技术发展趋势建立了网络安全边际收益曲线模型,使用该模型对战略转移网络安全责任的政策方向进行了判断,对战略政策措施进行了分析,最后提出了针对中国网络安全空间责任分配政策的建议。

2 战略主要内容框架

目前大多数私营部门出于自身商业利益的考虑,都会主动测试其产品的网络安全性。但当产品安全问题的修复成本较高时,出于缩短生产周期、快速发布产品抢占市场的考虑,一般不会为此采取额外的预防措施。同时,在美国现行的法律体系下,私营部门缺少增强产品网络安全性、将网络安全缺陷成本内部化的动力。尚没有任何机制让私营部门对其产品使用过程中因安全缺陷产生的网络安全成本负责。2021年5月美国最大的燃油管道系统运营商 Colonial Pipeline 遭受勒索病毒攻击。运营商启动预防措施,关闭了石油管道,严重限制了美国东海岸的汽油和航空燃料供应,其下游合作伙伴在此过程中遭受了重大经济损失^[3]。美国发生的网络安全事件表现出典型的市场外部性,一方面网络安全真实的成本在商品价格中没有得到充分体现,最终损害了终端用户的利益。另一方面私营部门受商业利益驱使,减少对产品网络安全的投资,最终使整个数字生态环境的安全性受损,安全事件频发。为了应对市场机制失灵的挑战,战略拟重塑市场力量,改变激励方式,在平衡网络空间责任方面做出根本性转变,使得数字生态环境中最有能力的一方担负更多的网络安全责任。在具体政策方面,战略采取了以下5项措施。

2.1 推动立法,对软件安全责任分配做出根本性改变

拜登政府上台后,美国接连发生了 SolarWinds^[1]、

Log4j^[10] 等因软件安全问题引发的网络安全事件,相关事件对美国国家安全产生了严重影响。因此,战略认为目前的市场机制,未能对私营部门施加足够的压力,导致其忽视最佳安全开发实践,发布了带有已知安全漏洞或不安全默认配置的产品。同时私营部门利用市场地位,通过合同完全免除安全责任,进一步降低了其遵守安全设计、测试、发布原则的意愿。最终导致了美国数字生态系统的系统性风险,并由政府和普通民众承担后果。为此战略计划与国会和私营部门合作制定法律,确定软件产品和服务的责任。在此过程中将吸取前期经验,防止私营部门通过合同条款逃避网络安全责任。为了对具体责任进行界定,战略拟制定软件开发安全标准,并将其命名为安全港框架,内容将借鉴美国国家标准与技术研究所(NIST)安全软件开发框架(SSDF)^[11]等当前软件开发最佳安全实践,同时为了应对受技术发展影响不断变化的网络安全形势,战略要求框架必须随时间推移而改进。

NIST 开发的 SSDF 是一套软件安全开发实践,该技术框架在组织结构、软件代码保护、软件安全质量管理、软件漏洞管理4个方面提出了67项软件开发最佳安全实践,涉及整个软件开发生命周期。遵守 SSDF 虽然对私营部门具有一定挑战性,但该框架为实体提供了一种兼具功能性和安全性的结构化开发途径。通过遵循其原则可以减少软件漏洞、增强软件安全性,最终开发出安全可信的软件产品。根据战略目前的计划,后期美国政府将推动立法,要求私营部门遵循安全港框架,承担软件制造过程中的网络安全注意义务,在法律层面重新平衡网络空间安全责任。

2.2 加强问责,迫使供应商切实履行网络安全责任

2022年9月14日,美国总统行政办公室根据《改善国家网络安全》行政命令的要求发布了 M-22-18 备忘录^[12],要求美国联邦政府各机构只能采购符合 SSDF 要求的软件及服务,私营部门向美国联邦政府机构提供的产品及服务在软件全生命周期各环节必须符合 SSDF 的67项最佳安全实践。但备忘录只要求私营部门使用自证的方式证明其产品符合 SSDF 要求。在美国联邦政府机构检测软件安全质量时,提供产品符合安全软件开发实践的证明材料即可。这种自证安全的方式并不能保证私营

部门如实报告真实情况,为此战略要求私营部门向美国联邦政府提供软件及服务时,必须遵守其做出的合同承诺,即所提供的产品是在严格遵守 SSDF 要求的前提下生产、发布的。美国司法部将按照《民事网络欺诈倡议》^[13],根据《虚假申报法》^[14]对未能履行网络安全义务的私营部门提起民事诉讼,追究其故意提供有缺陷的网络安全产品或服务、歪曲网络安全实践真实情况,使美国联邦政府信息系统面临风险的责任。民事网络欺诈倡议发布于 2021 年,旨在打击美国联邦政府供应商网络安全相关欺诈的行为,是美国司法部应对网络威胁的民事执法工具。战略在网络最佳安全实践问题上对《民事网络欺诈倡议》的引用,将借助联邦政府采购市场的力量,迫使私营部门按照网络安全最佳实践提升软件及服务安全质量,提升美国数字生态环境整体的安全性。

2.3 保护个人数据,让数据管理者承担数据保护责任

随着人类社会对互联网依赖程度的加深,公众在使用个人设备进行购物、浏览、工作或使用穿戴设备时产生了大量包括生物特征数据在内的个人数据,而负责提供相关应用的公司会在后台收集个人数据,并使用这些数据开展消费行为预测、个性化定价、定向广告推送等与公众期望不符的业务。此外,当收集数据的公司没有对数据进行妥善管理时,个人信息可能被不法分子盗取并买卖,最终导致欺诈、歧视和诱导性消费等情况,对消费者的个人利益造成严重伤害。当前美国在国家层面涉及个人信息收集和使用的法律主要为 1974 年的《隐私法》^[15]以及 2002 年的《电子政务法》^[16],法律的制定时间较为久远,已不能很好地解决 20 余年后个人数据安全面临的问题。为了保护个人数据,降低个人数据被恶意使用、盗取的风险,战略拟通过立法对收集、使用、传输和维护个人数据的行为做出明确的限制,并对个人地理定位、健康状况等敏感数据做出可根据外界威胁情况调整的强有力保护措施,让个人数据管理者切实承担起保护个人数据的责任。

2.4 继续借助政府采购力量,平衡物联网网络安全责任

近年来物联网设备在个人电子消费、工业生产、城市交通和健康监测等多个领域得到广泛的应用,

在设备数量大幅增长的同时,由于美国前期缺乏统一的网络安全行业标准且受到商业利益的影响,物联网产品的网络安全并未得到私营部门的重视,攻击者可通过入侵物联网设备,开展敏感数据窃取、大规模物联网僵尸网络攻击、传播恶意软件等多种非法活动。为提升物联网设备安全性,战略计划继续按照 2020 年《物联网网络安全改进法案》^[17]要求,通过联邦研发、采购和风险管理工作改善物联网网络安全,同时继续推进“改善国家网络安全”行政命令中物联网安全标签计划的实施^[1]。

《物联网网络安全改进法案》要求 NIST 制定新的物联网设备安全指南,美国白宫管理和预算办公室(OMB)根据指南颁布新的规则并修订《联邦采购条例》^[18],对美国联邦政府所采购物联网设备的最低网络安全标准做出要求,禁止联邦政府机构购买不符合标准的物联网设备。而物联网安全标签计划则是按照《关于改善国家网络安全的行政命令》开展的面向消费者的一项计划。NIST 已按照《关于改善国家网络安全的行政命令》的要求于 2022 年 2 月 4 日发布了《消费类物联网产品网络安全标签推荐标准》^[19],对物联网产品应符合的网络安全标准、标签的设计和标签认证方式做出了要求,为计划的实施做好了准备。该计划 2024 年启动,实施后可使消费者在购买物联网产品时根据标签内容直观地了解物联网设备的网络安全性,推动消费者购买安全性更高的设备,同时激励私营部门满足更高的网络安全标准、鼓励零售商销售安全设备。这两项举措的共同之处是利用市场的力量对物联网网络安全责任进行再平衡,使物联网私营部门承担更多的网络安全责任,最终实现更加安全的物联网环境。

2.5 探索联邦网络保险制度,转移实体网络安全经济责任

目前有大量的社会实体依赖网络和信息系統开展日常工作,当业务因灾难性网络事故而被迫中止时,受害者不仅面临技术问题,还要面对经济上的困难。网络安全保险是一种日益重要的风险转移机制,在加强网络安全和增强弹性方面具有重要作用^[20]。在美国商业网络保险方面,网络保险市场的直接承保保费已从 2015 年的 14 亿美元增长至 2021 年的 65 亿美元^[21]。在近年发生的多起勒索软件攻击事件中,网络保险公司为投保人支付了赎金,

起到了应有的作用,但频发的勒索事件同时导致了保费的上涨。2021年美国网络保险直接承保保费较上年增长94.7%,但独立保单总数较2020年仅增长31.8%^[21]。为了让无力支付投保费用的公司可以购买网络保险,拜登政府的战略首次提出对联邦网络保险制度进行探索,期望这种保险制度可以在灾难性网络事故发生时为实体提供经济方面的稳定支撑,转移网络安全经济责任,防止社会出现系统性金融风险。

3 美国网络安全责任政策的合理性和有效性分析

为了建设可防御、有弹性的数字生态环境,应对市场机制失效问题。战略拟通过改变政府在网络安全治理中的角色,加强对市场的监管,重新分配网络空间责任。本文通过网络安全边际成本模型对战略政策转向的合理性进行了判断,对政策具体措施的有效性进行了分析。

3.1 合理性分析和政府角色分析

近年来网络安全经济迅速增长,网络安全产业根据业务的不同演化出了完整的产业链,在产业链的上下游形成了包括基础硬件安全、软件系统安全、安全算法研究、网络安全设备研发和网络安全软件开发等各类专业团队,专业化的分工在提升网络安全防护能力的同时,提高了网络安全经济的生产力,降低了网络安全防护的成本。假设目前网络安全活动参与者的行为是理性的,当网络安全的增量收益超过增量成本时,参与者将追求扩大网络安全的规模。其他条件不变时,参与者可能会以更高的成本开展网络安全活动,例如,对于缺少安全维护的系统,加强其安全性可以采用自动化漏洞及安全扫描程序,但提升高安全等级系统的防护能力时,需要采用人工渗透测试或编写代码等更加耗时、成本更高的方式开展安全测试工作。所以,开展安全工作的成本曲线向上倾斜,而随着网络安全工作的不断开展,信息系统得到了更好的防护,网络安全收益也随之降低,网络安全收益曲线将向下倾斜(如图1所示)。此外根据现状,本文假定边际成本曲线的斜率高于边际收益曲线的斜率。在整个市场中,需求由保护信息系统所带来的收益决定,供给由保护系统所需的成本决定,这两条曲线的交点决定社

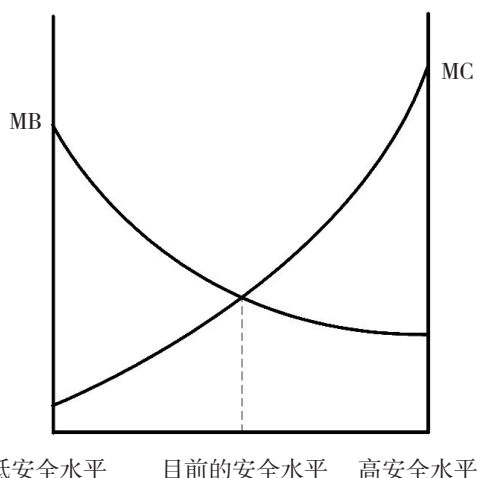


图1 网络安全收益及成本曲线

注:MB代表网络安全边际收益曲线,MC代表网络安全边际成本曲线;图2同。

会网络安全总体水平。

边际收益曲线和边际成本曲线的位置受到社会信息化水平、网络安全技术水平和法律法规的变化影响,例如,人工智能技术在网络安全中的应用、网络安全人才的培养都会降低社会网络安全成本,从而使代表供给的网络边际成本曲线向右下方移动。相比之下,对网络安全实行更严格的监管措施,社会重要基础设施网络信息化程度提升,网络用户数量上升,会使代表需求的网络安全边际收益曲线向右上方移动。上述两种曲线的移动方式都会使曲线的交点向右侧移动,代表社会整体网络安全程度的提升,如图2所示。根据上述分析,美国网络安全战略方向是否正确,是否可以提升数字生态环境整体安全水平,取决于其是否可以有效提升网络安全边际收益,降低网络安全边际成本。

按照Samuelson^[22]提出的公共物品理论,网络安全属于一种具有强公共利益特征的私人商品,主要由私人利益相关者以一定的成本提供,如表2所示。

当这种商品的成本满足社会对网络安全的需求时,会为产业赋能、促进就业、提升社会生产效率。当商品的安全投入成本不能满足需求时,会对社会造成直接(如由网络安全事件导致的设备损坏、数据丢失)、间接(如预防措施)和隐形(由于对网络系统信任度降低而导致的生产效率下降)等类型的损失。目前网络安全,特别是作为主要组成部分

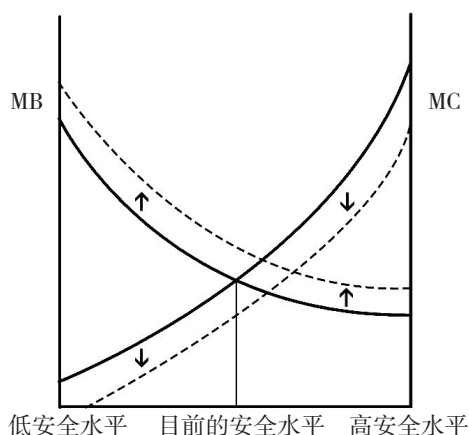


图2 移动后的网络安全收益及成本曲线

表2 物品属性分类表

类别	非竞争性	竞争性
非单独占有	如国防、空气等	如游乐场、城市道路等
单独占有	如健身房用品、电影院等	如私人物品、汽车、网络安全等

的软件安全在美国历来具有特殊的法律地位，商品网络安全缺陷很少成为责任诉讼的法律基础，私营部门也很少为自身商品负外部性产生的损失承担责任。这导致私营部门在确定其商品的安全成本时，所依据的往往是商业信誉、收入效应等个人可以感知的成本，而非消费者成本、社会成本等公共利益。其商品的网络安全成本并没有完全被商品的制造者吸收，并随着商品的销售被放大，最终由整个社会承担。这种负外部性的存在，转移了应由私营部门承担的网络安全责任，使数字生态环境中私营部门的网络安全收益边际曲线向图2左下方移动，导致其缩减网络安全投资，偏离社会实际网络安全需求，让整个数字生态环境的安全性低于社会预期。虽然市场具有自我调节能力，但是在网络安全领域由收入、声誉构成的激励作用过于弱小，不足以使私营部门充分提高其网络安全投资至社会需要水准，解决数字生态环境中安全漏洞大量存在的问题。重大网络安全事件的频发已经证实了美国现有网络安全管理制度下的市场失灵现象。为了应对网络安全的负外部性问题，政府应将网络安全视为如国防一样的公共产品进行管理，通过制定法律、加强监管等方式综合运用政策工具，提升私营部门产品的安全

性。美国网络安全战略拟转变网络空间责任分配方式，重新平衡网络空间责任，通过加大产品网络安全缺陷处罚力度、推广网络安全保险制度等措施激励私营部门加大网络安全投资。在理论上可以提升美国社会的网络安全需求，使边际收益曲线向图2的右上方移动，提升社会整体安全水平，引领美国数字生态环境走向更加安全的未来。

3.2 有效性分析和现有实施障碍

通过法律法规建设加强监管，将使私营部门投入更多的资源、时间增强产品的网络安全性，承担更多网络安全责任。同时，会带来产品成本的增加、价格的上涨。价格上涨的幅度与监管施加的责任力度成正相关关系，过高的产品价格将导致产品销量下降、创新减缓、就业岗位减少和税收收入降低等多种问题。同时过于严格的责任制度会形成技术和财务壁垒，使行业内中小企业因缺少资源难以参与市场竞争。而偏弱的监管强度无法激励私营部门在产品安全方面投入更多资源。

因此，在明确网络安全责任相关政策的方向后，还应注意具体政策的监管力度，适当的政策才能在实现转移安全责任、建设良好数字生态环境的同时促进产业健康发展。战略对此也给予了特别的关注。在软件安全责任方面，战略认为安全漏洞对于软件是不可避免的，软件公司应拥有创新的自由。在生产产品时，软件制造商应履行基于软件开发安全标准的注意义务，政府为此推动开发的安全港框架同样是为了保护履行注意义务的软件制造商。在美国法律体系中，民事责任的界定可以采用严格责任和疏忽责任的形式，在严格责任下责任实体无论其自身行为如何，如果产品出现问题都要承担责任。美国对汽车行业采取的就是严格责任。考虑到软件产品相对于汽车的复杂性和非标准性，战略采取疏忽责任的形式，即实体只有在未能满足软件开发安全标准时才承担责任。在具体安全开发实践标准上，战略参考的SSDF也只是对软件全生命开发周期各阶段的注意事项给予了示例指导，将实施的细节留给软件制造商自行决定，软件制造商可以选择成本最低的方式进行软件的设计开发。在美国联邦政府软件采购方面，战略仍然保留了M-22-18备忘录中由软件制造商自证安全的方式，为其降低生产成本。在增强物联网安全方面，为了适应产品的多样性，降低物联

网厂商满足法规付出的安全成本,《消费类物联网产品网络安全标签推荐标准》在定义产品安全基线时只规定各环节期望达到的安全效果,具体实现方式由物联网厂商自行确定。战略在转移安全责任的同时,考虑了网络安全相关行业的复杂性和多样性,根据行业特点,在制定安全标准时给予私营部门一定的空间,尽力保护私营部门的生产积极性。

虽然战略在降低因责任转移而产生的安全成本方面采取了多项措施,但在各项措施落地实施方面,仍存在较多不确定性。在软件安全责任方面,由包括微软、SAP、甲骨文和IBM等40余家大型国际软件公司组成商业软件联盟(BSA)对战略的出台反应平淡^[23],认为战略是经过深思熟虑的,并表示软件制造商将认真对待客户和公众的责任,将与政府合作推进共同优先事项,以产生最大利益。2021年11月,BSA向NIST发送的关于SSDF的回复意见中建议^[24],NIST应指导软件实体遵循BSA安全软件框架。BSA认为NIST对落实SSDF所产生的成本考虑不足,应该让软件开发人员以更具成本效益和创新的方式满足机构的安全要求。同时,对SSDF所采取措施的有效性、验证符合SSDF要求的方式和监管措施匹配技术进步速度的能力等问题表示疑虑,认为SSDF的要求可能在增加成本的同时并不会提升软件安全性。《物联网网络安全改进法案》由于仅适用于美国联邦政府采购的物联网相关设备,而物联网产品网络安全标签计划则由物联网设备自行决定是否参与计划,并非强制要求。因此物联网相关责任转移的措施并未导致设备制造商的强烈质疑。同时,相关措施对改善数字生态环境安全的成效仍有待观察。

4 启示

目前中国金融、能源、军事和政府机构等关键基础设施对网络的依赖程度日益加深,网络安全关乎国家安全和社会稳定。随着中国《网络安全法》的发布,网络安全等级保护制度以及关键信息基础设施安全保护条例的实施,中国网络安全水平有了较大提升。但截至2024年7月,尚没有法律对软件制造、信息技术服务、物联网等领域因产品网络安全负外部性导致的责任进行明确划分,在推广网络安全保险方面也处于试行阶段。为了建设良好的数字生态环境,中国应在转移网络安全责任方面采取

措施,让处理网络安全问题更具经济效率的各行业厂商承担更多的责任,这样才能建设中国更加安全的数字生态环境。在具体措施方面,本文建议如下:

(1) 以结果为导向,制定产品全生命周期安全标准。

为了让国内各行业私营部门能切实承担网络安全义务,中国应由国内科研机构牵头制定相关行业网络安全标准。在标准的制定过程中应积极听取来自产业代表、学术机构、科研机构和消费者代表等多方利益相关者的意见。在标准内容方面,为减缓因行业技术进步速度较快导致标准过时的问题,增强标准应对不同产品的适应性。在制定标准内容时,不应效仿SSDF,为软件安全开发的具体流程做出指导。应使用期望的安全结果代替具体实现过程,让制造商及服务提供商自行选择最适合的方式完成满足标准要求的目标。另外,在制定标准时除参照最佳安全开发实践建立软件全生命周期管理体系外,应聚焦于网络安全领域的关键问题。例如,在软件安全漏洞管理方面,应要求负责开发的私营部门维护其产品软件物料清单,详细记录产品所使用的组件名称、版本,并根据清单内组件的漏洞情况,对较易被攻击者利用的高风险漏洞予以修复。在软件开发环境安全方面,除确保开发环境安全可靠外,还应使用来源可验证的开发工具,定期开展开发工具的安全性分析。标准应更多地聚焦于对数字生态环境造成较大影响的关键问题,明确私营部门在产品全生命周期中应尽的义务,在降低合规成本、保护行业生产积极性的同时,改善数字生态环境安全。

(2) 推动立法,让行业实体承担更多的网络安全责任。

完成行业网络安全标准的制定后,应通过立法要求开展相关生产活动的私营部门按照标准开展生产活动,在产品全生命周期履行网络安全注意义务。当私营部门因未能履行其网络安全注意义务,给产品购买方造成损失时,应向产品购买方进行赔偿。追究责任的范围应仅限于最终制造产品和提供服务的一方,产品中开源代码的提供者应不予追究责任。同时在制定法律时应避免制造商及服务提供商通过合同及市场地位免除自身的网络安全责任。

(3) 继续推广网络安全保险,转移网络安全经济责任。

在完成立法的同时,为避免市场中的一方因网

络安全事件所产生的经济影响而面临困境,可以通过网络安全保险制度,对其经济责任进行转移。市场中的产品制造商、服务提供商以及消费者应均可购买网络安全保险,当产品制造商、服务提供商因未能履行网络安全注意义务而面临赔偿时,可由保险公司向受害人进行赔偿。当其已履行了注意义务,但仍导致消费者利益受损时,相关损失可由消费者购买的网络安全保险进行赔偿。在产品制造商、服务提供商投保时,网络保险机构还可以要求保单持有人遵循最佳网络安全实践,降低其遭受网络攻击的风险。

(4) 建立网络安全标签制度,通过市场力量推动网络安全。

为配合网络安全保险制度的落实,可对我国 ICT 产品网络安全标签制度进行探索。由国内保险行业建设网络安全防护能力测试平台,对各设备制造商、服务提供商的产品开展网络安全评测,并使用不同安全等级对其产品进行标识。安全等级较低的产品应禁止在中国政府机关、军队、科研院所以及关键基础设施中进行使用。同时在确定设备制造商、服务提供商网络安全保险投保费用时,可将其产品的网络安全等级作为重要参考指标。■

参考文献:

- [1] 张焯阳,刘蔚.美国《改善国家网络安全的行政命令》政策理念初探[J].全球科技经济瞭望,2022,37(8):9-15.
- [2] Cyber Safety Review Board. Review of the summer 2023 Microsoft Exchange online intrusion[EB/OL]. [2024-03-20]. https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf.
- [3] EASTERLY J, FANNING T. The attack on colonial pipeline: what we've learned & what we've done over the past two years[EB/OL]. [2024-03-20]. <https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years>.
- [4] BIDEN J R, Jr. National security memorandum on improving cybersecurity for critical infrastructure control systems[EB/OL]. [2024-03-20]. [https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-](https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/)
- [cybersecurity-for-critical-infrastructure-control-systems/](https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/).
- [5] BIDEN J R, Jr. National Cybersecurity Strategy[EB/OL]. [2024-03-20]. <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>.
- [6] European Parliament. European Parliament legislative resolution of 12 March 2024 on the proposal for a directive of the European Parliament and of the Council on liability for defective products[EB/OL]. [2024-03-20]. https://www.europarl.europa.eu/doceo/document/TA-9-2024-0132_EN.html#title2.
- [7] European Parliament. Defective products: revamped rules to better protect consumers from damages[EB/OL]. [2024-03-20]. <https://www.europarl.europa.eu/news/en/press-room/20240308IPR18990/defective-products-revamped-rules-to-better-protect-consumers-from-damages>.
- [8] Great Britain Parliament. Product Security and Telecommunications Infrastructure Act 2022[EB/OL]. [2024-03-20]. <https://www.legislation.gov.uk/ukpga/2022/46/introduction/enacted>.
- [9] Australian Government. 2023–2030 Australian Cyber Security Strategy[EB/OL]. [2024-03-20]. <https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf>.
- [10] Cyber Safety Review Board. Review of the December 2021 Log4j Event[EB/OL]. [2024-03-20]. <https://www.cisa.gov/sites/default/files/2023-02/CSRB-Report-on-Log4j-PublicReport-July-11-2022-508-Compliant.pdf>.
- [11] National Institute of Standards and Technology. Secure Software Development Framework (SSDF) Version 1.1[EB/OL]. [2024-03-20]. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf>.
- [12] Office of Management And Budget. Enhancing the security of the software supply chain through secure software development practices[EB/OL]. [2024-03-20]. <https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf>.
- [13] U.S. Department of Justice. Deputy attorney general Lisa O. Monaco announces new civil cyber-fraud initiative[EB/OL]. [2024-03-20]. <https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative>.

- [14] U.S. Department of Justice. The False Claims Act[EB/OL]. [2024-03-20]. <https://www.justice.gov/civil/false-claims-act>.
- [15] U.S. Department of Justice. Privacy Act of 1974[EB/OL]. [2024-03-20]. <https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1279>.
- [16] U.S. Department of Justice. E-Government Act of 2002[EB/OL]. [2024-03-20]. <https://www.justice.gov/opcl/e-government-act-2002>.
- [17] The Senate and House of Representatives of the United States of America. IoT Cybersecurity Improvement Act of 2020[EB/OL]. [2024-03-20]. <https://www.congress.gov/bill/116th-congress/house-bill/1668>.
- [18] General Services Administration. Federal Acquisition Regulation[EB/OL]. [2024-03-20]. <https://www.acquisition.gov/sites/default/files/current/far/pdf/FAR.pdf>.
- [19] National Institute of Standards and Technology. Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products[EB/OL]. [2024-03-20]. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-2.pdf>.
- [20] Federal Insurance Office, U.S. Department of The Treasury. Annual report on the insurance industry[EB/OL]. [2024-03-20]. <https://home.treasury.gov/system/files/311/FIO-2021-Annual-Report-Insurance-Industry.pdf>.
- [21] National Association of Insurance Commissioners. Report on the cyber insurance market[EB/OL]. [2024-03-20]. <https://content.naic.org/sites/default/files/cmte-c-cyber-supplement-report-2022-for-data-year-2021.pdf>.
- [22] SAMUELSON P.A. The pure theory of public expenditure[J]. The review of economics and statistics, 1954, 36(4): 387-389.
- [23] BSA. BSA comments on national cyber strategy, looks forward to working with administration[EB/OL]. [2024-03-20]. <https://www.bsa.org/news-events/media/bsa-comments-on-national-cyber-strategy-looks-forward-to-working-with-administration>.
- [24] BSA. BSA Comments on the NIST Secure Software Development Framework Version 1.1[EB/OL]. [2024-03-20]. <https://www.bsa.org/files/policy-filings/11052021nistssdf.pdf>.

Analysis and Enlightenment of U.S. Cybersecurity Responsibility Policy

ZHANG Yeyang, LI Weiyi, HAN Yang, LI Xiang, XIA Chunzi, ZHANG Lei

(Institute of Scientific and Technical Information of China, Beijing 100038)

Abstract: In 2023, the Biden administration of the United States released the National Cybersecurity Strategy, which is based on Executive Order 14028 issued in 2021. It fundamentally changes the allocation of cyberspace responsibilities, emphasizing the role of government regulation in the market. By reshaping the market structure, cyber risks are transferred from end users to various corporate entities that own data and technology. Avoid end users from becoming the weakest link in cyberspace due to the lack of professional personnel, data, technology and other resources, and let the participants who are most capable of ensuring cybersecurity shoulder the corresponding responsibilities to build a defensible and resilient digital ecosystem. Starting from the background of the strategy, this paper analyzes the measures to balance cybersecurity responsibilities, and then establishes a cybersecurity marginal benefit curve model, which is used to judge the rationality of the policy direction for strategic transfer of cybersecurity responsibilities, and analyze the effectiveness of specific policy measures of the strategy. Finally, suggestions for the distribution policy of cybersecurity space responsibilities in China are proposed.

Keywords: cybersecurity responsibility; cybersecurity strategy; digital ecosystem; cyber insurance