

世界各国网络安全战略分析与启示

李欲晓¹, 谢永江²

(1. 中央网络安全和信息化领导小组办公室, 北京 100010;
2. 北京邮电大学互联网治理与法律研究中心, 北京 100876)

摘要: 国家网络安全战略是一国网络安全的顶层设计和战略框架, 体现了国家安全、危险管理和用户保护三位一体。目前世界上主要发达国家均制定了国家网络安全战略。我国应当借鉴世界网络发达国家的经验, 制定我国的网络安全战略。其内容应包括网络态势评估、战略目标、战略行动、网络治理体制和机制等。

关键词: 网络; 网络安全; 战略

中图分类号: D922.1

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00017

Analysis and enlightenment on the cybersecurity strategy of various countries in the world

LI Yu-xiao¹, XIE Yong-jiang²

(1. Office of the Central Leading Group for Cyberspace Affairs, Beijing 100010, China;
2. Institute of Internet Governance and Law, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: National cybersecurity strategy is the top-level design and strategic framework of the country, which includes the national security, risk management and the personal protection. Now the main developed countries in the world have made the national cybersecurity strategy. So the strategy of our country drawing lessons from the experience of the developed countries should also be enacted. And the strategy should include the cybersecurity situation assessment, strategic target, strategic actions, the system and mechanism of internet governance, and so on.

Key words: network, cybersecurity, strategy

1 引言

网络安全是网络空间状态的一种期望目标, 即网络空间风险降低到可接受的最小程度^[1]。战略是为实现长期或总体目标而制定的行动计划^[2]。各国普遍认为, 网络安全是影响社会各个层面的战略性国家问题。制定国家网络安全战略是提升国家基础设施和服务安全性、可恢复性的重要手段^[3]。它是一国网络安全的顶层设计和战略框架, 通过确立全国性的网络安全战略目标, 并规定一系列在一定时间内应予完成的优先任务, 以提升国家的网络安全

全, 体现了国家安全、危险管理和用户保护三位一体。我国 2015 年 7 月公布的《网络安全法》草案专设一章“网络安全战略、规划与促进”, 足见国家对网络安全战略的重视。本文通过对世界各国网络安全战略进行分析, 发现网络安全战略的一些规律性内容, 以期有益于我国网络安全战略的制定。

2 各国网络安全战略简要分析

2.1 各国网络安全战略制定概况

自从 2000 年俄罗斯出台《网络信息安全学说》、2003 年美国制定《确保网络空间安全的国

收稿日期: 2015-12-07; 修回日期: 2015-12-29。通信作者: 谢永江, xieyongjiang@bupt.edu.cn

基金项目: 工程院重大战略咨询基金资助项目 (No.2015-ZD-10)

Foundation Item: Major Consultant and Research Project of Chinese Academy of Engineering (No.2015-ZD-10)

家战略》以来,截至 2015 年 8 月,世界上已有 64 个国家制定了网络安全国家战略^[4,5],其中除了俄罗斯、美国少数国家的网络安全战略制定于 2010 年前外,绝大多数国家的网络安全战略均在 2010 年之后密集出台。另有希腊、巴基斯坦、沙特阿拉伯等国家的网络安全战略正在制定中。经济合作与发展组织的 34 个成员国中,只有 7 个国家没有制定网络安全战略(没有制定网络安全战略的国家为智利、希腊、冰岛、以色列、墨西哥、葡萄牙、斯洛文尼亚)。欧盟 28 个成员国中,只有 6 个国家没有制定网络安全战略(没有制定网络安全战略的国家为保加利亚、克罗地亚、希腊、马耳他、葡萄牙、斯洛文尼亚)。此外,欧盟作为一个国际组织,也在 2013 年制定了欧盟网络安全战略;美国和俄罗斯还出台了网络安全国际战略。可见,除了中国外,世界上网络大国或网络发达国家几乎都制定了网络安全国家战略。

各国网络安全战略之所以如此密集地出台,主要是因为随着互联网的迅速发展和普及,各国政府、关键基础设施、企业和公民均严重依赖于网络的可靠功能。网络安全出现问题,将严重危及政府和企业的运转,极大影响公众的社会生活。可以说,网络安全是一国繁荣发展的“生命线”。就像美国《确保网络空间安全的国家战略》所指出的那样:“网络是(关键基础设施的)神经中枢——我国的控制系统。网络空间包括成千上万连接在一起的计算机、服务器、路由器和光缆,至关重要的基础设施依赖于它们来工作。因此,网络的正常运转对经济和国家安全都是必不可少的。”确保网络空间的可用性以及网络空间数据的完整性、真实性和保密性已经成为 21 世纪的重要课题。

2.2 各国网络安全战略基本内容

分析比较各国网络战略的主要内容,一般包括以下几个方面。

2.2.1 网络态势评估

各国网络安全战略基本上首先都要对网络发展形势进行评判,并对本国所面临的网络威胁进行评估。只有在正确评估的基础上,才能制定符合本国国情的网络安全战略。这种评估一般包括两个方面。

一方面是对网络的依赖性。政府、企业、社团和公民已经严重依赖互联网所提供的便利和创

造的机会。互联网支撑着国家的经济发展、社会进步和人民生活水平的提高。

另一方面是面临的网络安全威胁。对网络的依赖日益加重使各国存在被网络攻击的潜在漏洞。网络产品和服务发生故障、信息基础设施损坏以及严重的网络攻击可以给政府、企业和公民带来极大损害,甚至影响一国的社会生命线。各国纷纷将网络安全威胁列入国家安全的优先事项。法国更是明确将网络安全与核威慑、弹道导弹、弹道导弹战略核潜艇和攻击核潜艇并列,均属于为维持战略上和政治上的国家自治所必需的优先发展项目。

2.2.2 战略目标

国家网络安全战略主要是为国家网络安全政策提供一个顶层设计框架,明确和引导各项行动和计划,以增强国家网络空间的安全态势,指导有关网络空间安全的行动。各国的网络安全战略目标核心内容大同小异。总的目标大体是建设一个世界领先的(主要针对网络发达国家)、安全的、稳定的、可恢复的、可信的、有活力的网络空间。

总目标可以化为若干个具体目标。具体目标通常包括制定网络防御政策、建设网络防御能力、实现网络可恢复性、减少网络犯罪、支持网络安全产业发展、保护关键信息基础设施等。

2.2.3 战略行动

各国网络安全战略除了规定战略目标外,还会规定实现战略目标拟采取的具体行动和措施。由于网络空间不断发展,网络安全形势也不断变化,需要持续地跟踪评估,因此各国网络安全战略行动一般都有一个时间限制,一般是 3~5 年。之后要根据网络安全形势的变化进行不断调整,因此网络安全战略是一个“活文件”^[3]。

各国网络安全战略行动一般包括以下几个方面。

1) 提高侦测、预防、阻止和处置网络攻击风险的能力,控制网络犯罪。例如,英国网络安全战略优先行动之一是继续提高察觉和分析尖端网络威胁的能力;韩国提出要在国家层面侦测和阻止网络攻击。

2) 保护关键信息基础设施。关键信息基础设施几乎是所有关键基础设施的核心组件,并且变得越来越重要。因此关键信息基础设施的保护是各国网络安全的主要优先项。

3) 加强政府、企业和公众的合作。各国均认为, 政府部门的能力有限, 无力单独完成网络安全保护工作。因此, 需要政府、企业、社会公众同心协力, 各负其责, 共同维护网络安全。例如, 美国要求联邦政府致力于创立并将参与公共与私营部门之间的合作伙伴关系; 韩国提出要建立私人部门、公共部门和军事部门联合响应体系; 日本战略明确了政府、重要基础设施供应商、私营公司、教育机构和科研机构、个人用户、中小企业以及网络空间相关运营商的角色。

4) 加强能力建设, 开发自主可控技术。鉴于网络犯罪手段越来越复杂, 策划越来越精细, 有必要强化信息技术安全和关键基础设施保护的研究, 加强技术主动权和经济能力建设, 避免受制于人。例如, 美国提出要开发目前尚不存在的健全可靠的网络能力, 减少美国网络的脆弱性; 英国提出要推进有关网络安全专业技术的发展, 使英国继续保留优势地位; 法国提出要加强和保持法国的科学、技术、工业和人才能力, 以便维护自身的独立性。

5) 完善网络安全法律。法律是维护国家网络安全的重要手段。许多国家均提出要制定和完善网络安全法律法规, 反映技术进步和最新实践, 利用法律手段打击网络犯罪, 保护网络信息安全。例如, 英国提出要确保英国有一个强健的法律框架来使法律执行部门有效处理网络犯罪; 俄罗斯提出要完善俄罗斯联邦信息安全保障的法律基础。

6) 重视网络安全专业人才培养。网络安全专业人才是维护网络安全的关键。许多国家都非常重视网络安全人才的教育、培养和培训。例如, 美国将网络安全人才培训列入优先目标; 德国把加强联邦网络安全人员的培训作为实现安全战略的信息安全保障措施之一; 澳大利亚将推动网络安全熟练工人的培训作为战略优先项目; 俄罗斯将制定信息安全和信息技术领域人才培训的统一规定作为应当重视的任务之一。

7) 加强信息共享。实现网络安全应当基于综合手段, 这要求更加彻底的信息共享和协调。维护网络安全需要跨部门的合作, 因此信息共享成为协同行动的前提, 建设信息共享网络成为首选项。例如, 美国强调联邦、州、地方的信息共享和行业信息共享; 印度将信息共享合作作为实现

国家网络安全的策略之一。

8) 培养网络安全意识。网民是互联网治理的重要组成部分。网民的网络安全意识对国家网络安全战略的实施具有重要作用, 因此各国非常重视网民的网络安全意识培养。例如, 日本决定从小学、中学阶段开展增强网络安全意识的活动; 澳大利亚每年设网络安全意识周; 印度决定推动和发起综合性的有关网络空间安全的国家意识项目, 通过电子媒体持续开展安全素质意识和宣传运动, 帮助公民意识到网络安全的挑战, 管理、支持和帮助网络安全讲习班、研讨会和认证; 韩国设立国家“信息保护日”, 在小学、初中和高中阶段加强网络安全教育, 以便提高公众意识和扩大网络安全领域的基础。

9) 加强国际合作。网络空间是无国界的空间。各国均认识到, 加强国际合作是维护网络安全必不可少的条件。例如, 美国将国际网络空间安全合作作为优先目标之一; 英国将寻求国际合作来发展规范网络空间行为的国际规范和准则作为优先行动之一。

2.2.4 组织保障

维护网络空间安全需要一个强有力的领导机构。各国对此均非常重视, 纷纷设立新的网络安全监管机构, 提升网络安全监管能力。例如, 美国组建了国土安全部; 英国建立了一个新的网络防御运行组织来整合网络方面的国防能力, 并新设立了一个全球运行和安全控制中心; 法国设立了网络与信息安全局; 德国为了优化所有政府部门之间的行动合作, 提高保护和应对 IT 突发事件响应措施的协调能力, 设立国家网络响应中心和国家网络安全委员会; 日本加强建设“国家信息安全中心”作为指挥标杆的功能, 在内阁设立网络安全战略本部; 韩国在国家网络安全中心下设立“国家网络威胁联合响应小组”; 印度设立 24×7 h 国家关键信息基础设施保护中心; 澳大利亚在《网络安全战略》中发挥重要作用的是两个新的相互支持的组织——澳大利亚计算机应急响应小组和网络安全行动中心; 俄罗斯更是强调维护网络安全的组织体系, 包括: 联邦总统、联邦会议的联邦委员会、国家杜马、联邦政府、联邦安全理事会、行政权力机构、联邦总统和联邦政府建立的跨部门国家委员会、俄罗斯联邦组成实体的执行机构、地方自治政府、司法机构、社团和民众等。

3 我国网络安全战略基本内容

通过比较和分析世界上主要国家的网络安全战略,可以认为,我国的网络安全战略应包括以下主要内容。

3.1 网络势态评估

我国网络安全战略首先要对网络发展形势进行评判,并对我国所面临的网络威胁进行评估,从而为战略的制定、执行和评估提供必要的决策信息。

一方面,应明确我国政府、企业、社团和公民已经严重依赖互联网所提供的便利和创造的机会。我国的经济和社会发展繁荣离不开互联网。2015年以来,国务院相继发布了《关于促进云计算创新发展培育信息产业新业态的意见》、《关于大力发展电子商务加快培育经济新动力的意见》、《关于积极推进“互联网+”行动的指导意见》、《关于促进大数据发展的行动纲要》等重要文件,大力拓展互联网与经济社会各领域融合的广度和深度,以图利用互联网推动经济提质增效和转型升级。这都表明,互联网成为最重要的经济社会增长剂,并具有不可替代的作用。这就是习近平主席所说的:“没有信息化就没有现代化。”

另一方面,这种对网络的依赖也暴露了我国网络安全措施的不足,国家安全存在被网络攻击的潜在危险。关键信息基础设施发生故障、损坏以及遭受严重的网络攻击都可以给政府、企业和公民带来极大损害,甚至影响我国的政治安定、经济发展和社会进步的生命线。2013年“斯诺登事件”也暴露了我国网络安全的脆弱性。这就是习近平主席所说的:“没有网络安全就没有国家安全。”网络安全战略应当对当前我国面临的境内外网络安全风险来源、性质、类型、后果等做出全面、清晰、准确的判断。

3.2 战略目标

我国的网民数量世界第一,无疑是网络大国,但还不是一个网络强国。2014年2月,习近平主席在中央网络安全和信息化领导小组第一次会议上强调,网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题,要努力把我国建设成为网络强国^[6]。在致首届世界互联网大会的贺信中,习近平主席提出,

要维护网络安全,共同构建和平、安全、开放、合作的网络空间。另外,《国家安全法》第25条明确提出,国家建设网络与信息安全保障体系,维护国家网络空间主权、安全和发展利益。因此,我国网络安全战略总目标可以表述为:建设一个世界领先、和平、安全、开放、合作的网络空间,维护国家网络空间主权、安全和发展利益。

总目标可以化为若干个具体目标。就我国而言,网络安全战略目标应包括:1) 侦测、评判、预防、阻止网络攻击;2) 保护关键信息基础设施安全,确保关键信息基础设施的安全运行;3) 确保以最快速度恢复网络正常运行,将网络威胁损失最小化;4) 确保网络信息安全,防止敌对势力利用网络宣传危害国家安全。

3.3 战略行动

网络安全战略的制定不是一劳永逸的,通常需要根据质量管理的“PDCA模型”(计划—执行—检查—处置)不断改进。我国网络安全战略行动实施期限可以设定为5年,应包括以下9个方面。

1) 提高侦测、预防、阻止和处置网络攻击风险的能力,预防和控制网络犯罪。

2) 保护关键信息基础设施。完善网络安全等级保护制度,明确关键信息基础设施运营者的安全责任。

3) 加强政府、企业和公众的合作,建立各方共同维护网络安全的有效机制。

4) 加强能力建设,开发自主可控技术。提升网络与信息安全保护能力,加强网络和信息技术的创新研究和开发应用,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。

5) 完善网络安全法律。目前,要尽快制定《网络安全法》、《个人信息保护法》、《网络信息服务管理法》、《电子商务法》、《电子政务法》等网络安全领域的基本法律,反映技术进步和最新实践,保护网络安全。

6) 重视网络安全专业人才培养。建设网络强国,要培养造就世界水平的科学家、网络科技领军人才、卓越工程师、高水平创新团队^[6]。国家应完善网络安全人才教育培养体系和培训体系,建立有利于网络安全特殊人才成长的培养方案和奖励制度。

7) 加强信息共享。我国应建立国家网络安全

信息共享平台，协调优化配置资源，调动一切力量应对网络安全威胁。

8) 培养网络安全意识。顺应网络安全需要，我国从 2014 年开始设立了“国家网络安全宣传周”，但这远远不够。培养网络安全意识应当从占网民总数四分之一的学生抓起^[7]，在国民教育中建立完善的网络安全意识培养机制。

9) 加强国际合作。网络空间无国界。要本着相互尊重、相互信任的原则，深化国际合作，共同构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的国际互联网治理体系。

3.4 网络治理体制和机制

高效的网络治理体制和机制是网络安全战略目标得以实现的组织保障。这一治理结构应包括政府、企事业单位和社会公众的共同参与。

我国近年先后设立中央网络安全与信息化领导小组办公室和国家互联网信息办公室，这是顺应了网络安全发展态势的要求。目前我国已经基本形成了网信办负责顶层设计和统筹协调，工信部负责行业管理，公安部负责打击网络违法犯罪，国信办负责网络信息内容管理，其他部门在各自职责范围内分工负责“1+3+X”的网络监管体制。为了保障网络空间的有效治理，应该建立高效的统筹协调机制和可信信息共享机制，并以法律的形式对各部门的职责权限以及统筹协调、信息共享机制予以明确。

除了政府部门外，有关企业、科研机构、社会组织和社会公众在参与网络治理与网络安全保障方面的权利、义务和责任也应明确，形成一个各方共同参与的、可信可控、共享共治的网络安全保障机制。

3.5 关于网络安全国际战略

目前，世界上大多数国家都只制定了网络安全国家战略，而美国和俄罗斯在网络安全国家战略之外，还出台了网络安全国际战略。美国在 2011 年出台了《网络空间国际战略》；俄罗斯于 2013 年出台了《俄罗斯联邦国际信息安全国家政策基本原则》。美俄出台网络安全国际战略的目的主要在于，推销自己的战略意图和价值观，谋求制定网络空间国际治理规则的主动权，构建有利于其国家利益的网空间国际秩序。

我国作为网络大国和未来的网络强国，也应考

虑在制定网络安全国家战略的同时，出台国际战略，积极主动参与网络空间国际治理规则的制定，以维护我国网络空间主权，实现我国国家利益的最大化，确保我国由网络大国顺利发展成为网络强国。

4 结束语

网络空间作为继陆地、海洋、天空、太空之后的第五大空间，已经成为大国博弈的新领域。如美国，其早已在网络信息技术、网络空间规则、网络人才储备等方面进行了战略布局。我国作为网络后起大国，也应当及时跟进，尽快出台网络空间国家战略和国际战略，协调政府、企业和社会公众的力量，确保国家的网络空间安全和利益。

参考文献：

- [1] 德国网络安全战略[R]. (2011-02-23). Cyber Security Strategy for Germany[R]. (2011-02-23).
- [2] Oxford English dictionary[M]. Oxford: Oxford University Press, 2012.
- [3] European Network and Information Security Agency. National cyber security strategies: setting the course for national efforts to strengthen security in cyberspace[R]. 2012.
- [4] 北约合作网络防御卓越中心. 网络安全战略文件[EB/OL]. (2015-08-03). <https://ccdcoc.org/strategies-policies.html>. CCDCOE. Cyber security strategy documents[EB/OL]. (2015-08-03). <https://ccdcoc.org/strategies-policies.html>.
- [5] 国际电信联盟. 国家战略[EB/OL]. <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies.aspx>. ITU. National strategies[EB/OL]. <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies.aspx>.
- [6] 习近平：把我国从网络大国建设成为网络强国[EB/OL]. (2014-02-27). http://news.xinhuanet.com/politics/2014-02/27/c_119538788.htm. XI Jin-ping: building the China from the big internet country to the power internet country[EB/OL]. (2014-02-27). http://news.xinhuanet.com/politics/2014-02/27/c_119538788.htm.
- [7] 中国互联网络信息中心. 第 36 次中国互联网络发展状况统计报告[R]. (2015-07-23). CNNIC. The 36th Statistical Report on Internet Development in China[R]. (2015-07-23).

作者简介：



李欲晓（1969-），男，安徽肥西人，北京邮电大学互联网治理与法律研究中心主任，主要研究方向为网络法与网络治理。

谢永江（1973-），男，江西抚州人，博士，北京邮电大学互联网治理与法律研究中心常务副主任、研究员，主要研究方向为网络法和经济法。