

俄罗斯“主权互联网法案”主要内容 及实施前景分析

由鲜举， 颀 靖， 江欣欣

(国家工业信息安全发展研究中心，北京 100040)

摘 要：俄罗斯推出的“主权互联网法案”因主张建立独立的互联网体系而引发国际社会广泛关注。为了解和掌握其独立互联网体系建设的思路和实施路径，笔者在搜集整理大量相关资料的基础上，结合多年积累，全面介绍了法案出台的背景以及相关内容，并对其未来的实施前景进行了预测分析，为我国相关部门进行网络建设提供参考和借鉴。

关键词：俄罗斯；独立互联网；主权互联网法案

中图分类号：D93 **文献标识码：**A **DOI:** 10.3772/j.issn.1009-8623.2019.06.003

2019 年 5 月 1 日，俄罗斯总统普京正式签署了《关于对联邦〈通信法〉和联邦〈信息、信息技术和信息保护法〉进行修订的第 90 号联邦法案》，对俄罗斯通信和信息化领域的两大基本法——《通信法》和《信息、信息技术和信息保护法》进行修订。因在修订过程中突出强调要拥有相对独立的互联网，以确保紧急情况下其网络系统能够安全、稳定、完整运行而备受关注，并被外界习惯性称为“主权互联网法案”。为便于理解和使用，本文在非特殊说明情况下，仍沿用这一称谓。

1 法案出台的背景

据法案提出者称，该法案的提出主要有以下两点考虑：

一是美国新出台的《国家网络安全战略》虽未明确提出可对俄罗斯实施“断网”，但该战略具有明显的“侵略特性”，且明确指出“利用网络空间实施攻击”可成为美国针对不友好国家实施制裁的手段，并已变为一种“现实可能”^[1]。法案提出者认为，美国新版《国家网络安全战略》处处体现了“以武力维护和平”的思想，俄罗斯会被“经常”

且“无证据”地指控为“黑客攻击发起者”。美国的这一态度，让俄罗斯不得不积极应对。

二是在现实中网络攻击已开始越来越多被用于军事政治等领域，成为一种有效打击手段。美国已明确将网络空间列为继陆、海、空、天之后的第五作战域，其他西方大国亦开始日益注重信息主导权和信息优势争夺。法案提出者在提交法案时称，2012 年叙利亚被从互联网上断开是“美国国家安全局组织的一项特殊行动”^[2]。2016 年西方互联网公司拒绝为克里米亚地区提供网络服务则让俄罗斯更加警觉。为了赢得未来战争，也为了避免西方对俄实施“断网”，俄政府认为有必要在网络空间加快布局，在增强网络安全防护能力的同时，提升“俄罗斯互联网”的独立性，以捍卫国家信息主权。

2 法案的主要内容

法案全文共 3 章：第一章主要是对《通信法》进行的修订，第二章介绍了对《信息、信息技术和信息保护法》的相关修订，第三章对法案不同条款的生效时间进行了说明。其主旨思想是要加强俄罗斯联邦境内信息通信网的安全建设，让俄罗斯拥有

第一作者简介：由鲜举（1970—），女，高级工程师，主要研究方向为网络安全，安全保密管理，俄罗斯经济、电子信息产业与技术。
收稿日期：2019-05-28

一个独立于国际互联网的信息基础设施——“俄罗斯互联网”，以确保俄罗斯通信运营商在无法接入国外互联网根服务器的情况下，保证其境内的网络系统仍可安全、稳定、完整地运行，维护俄罗斯在信息空间领域的国家利益^[3]。其核心内容主要集中在以下4个方面。

2.1 重新界定信息通信网络运行管理的主体及其职责

2.1.1 网络运行主体及其职责

此次修订案扩大了网络服务提供主体的范围，将通信网络、其他技术通信网络（通常是指用来保障生产活动及对生产过程实施技术管理的通信网络）、域名系统、路由交换节点的所有者和各种形式的实际持有者（包括组织和个人）全部列为俄罗斯信息通信网络的运行主体（以下简称“通信运营商”），由其具体负责俄罗斯境内信息通信网络的稳定、安全、完整运行，并增设专门条款明确了通信运营商的职责。

修订案要求，通信运营商必须按照要求在其网络中加装防范网络威胁的技术手段，并向有关部门提交相关技术手段加装的物理位置等信息。为了消除通信运营商顾虑，法案规定，若因加装技术防范手段而造成通信网络中断，通信运营商将不承担任何责任，也不会因此受到惩处。另外还规定，若因加装技术防范手段而导致通信运营商不能履行或未全部/未正当履行通信服务合同而产生违约成本，运营商可向政府相关主管部门申请补偿，但须提交补偿申请和相关技术防范手段运行的信息。

除此之外，修订案还明确了通信网络（包括跨境通信网络）所有权和使用权转让时通信运营商应尽的义务及相关政府部门的职责（如应按照规定提交通信网络的使用目的等信息，并按照规定流程和期限进行转让等），以及路由交换节点所有者和实际运营者在提供接入服务时应遵守的原则（如不得为不符合规定的网络系统提供接入服务等），并增加了通信运营商有义务配合有关部门（包括侦查和国家安全机关）开展工作的内容，规定为保障上述机构能够依法履行其职责，运营商须执行上述机构制定的要求，必要时应向其提供帮助。

2.1.2 管理主体及其职责

法案规定，俄罗斯联邦政府主管部门对“俄罗

斯互联网”的安全、稳定、完整运行负有监督、管理、协调职责。目前，这一职责主要由通信、信息技术和大众传媒监督管理局承担。

修订案明确了政府在确保“俄罗斯互联网”稳定、安全、完整运行方面应开展的工作，指出应尽快出台相关文件明确以下问题：“俄罗斯互联网”和公用通信网（包括电信网、广播电视网及其他无线电通信网^[4]）稳定、安全和完整运行的要求；防范威胁技术手段的加装流程、技术规范，以及运行管理、升级改造要求；俄公用通信网与相关网络进行信息交互的规则和流程等。同时，要加快研究和制定路由引导规则、路由交换目录清单等文件，以便在紧急情况下（如断网时）有效应对。

法案同时规定，为拥有并提升确保“俄罗斯互联网”安全、稳定、完整运行的相关技能，通信运营商应按照法律规定，定期组织有关人员进行演练，演练的具体科目、内容、推演进程及参演人员等亦由联邦政府相关主管部门确定。

2.2 加强紧急情况下的网络管理，明确管理流程和规范

2.2.1 紧急情况下实行“集中统管”

修订案将原《通信法》第六十五章的名称改为“在紧急情况和紧急状态下公用通信网络的管理”，并增设了在紧急情况和状态下对信息通信网络进行“集中统管”的相关条款。

为了识别和查明威胁，修订案允许政府部门对相关通信网络（包括公用通信网）实施监控，并规定威胁发生时政府相关部门应对公用通信网络实施“集中统管”，并向所有参与集中统管的组织（包括机构和个人）及时通报信息和无偿提供防范网络威胁的技术手段（包括设备和工具）。指出政府部门要加快制定紧急情况/状态下实行“集中统管”时各方须共同遵守的信息传输规则，以及对集中统管活动实施监督的相关流程等，并明确了实现“集中统管”的两种方式：一是加强对防范威胁技术手段的管理；二是向加装了防御技术手段的通信网络、技术通信网络、路由交换节点、跨境通信线路和国家域名系统的运营管理者下达指令。

2.2.2 “集中统管”的流程和规范

法案规定，当俄罗斯联邦信息通信网络和公用通信网络受到威胁时，首先应确定威胁种类；其次

要确定消除威胁的程序及措施，包括加强对防范威胁技术设备、工具/手段的管理，并根据需要进行授权等；第三，确定集中统管框架下各方协作的组织和技术要求，包括受理运营商补偿申请的流程和期限等；第四，由联邦政府相关主管部门对集中统管的技术可行性进行论证，并制定应对方案；第五，明确不通过防范威胁技术手段过滤即可进行信息分发的特殊情形和条件。

为了确保能够有效应对威胁，法案还规定，集中统管期间，所有参与者使用的用以执行集中统管相关指令的通信手段（包括工具和设备）必须安装在俄罗斯联邦境内，并指定“公用通信网监督和管理中心”负责相关信息的统计工作。

2.3 强化对信息访问及使用过程中的安全管理和保护

第 90 号修订案的主旨是要打造一个安全稳定的网络平台，其在对俄罗斯的网络建设进行规范的同时，也强调要加强信息保护。

2.3.1 使用网络系统时的信息保护

修订案规定，为实现与公民、组织间安全的电子交互，联邦及地方政府部门、国有企业及相关机构应制定相应的规则和准则，并视情况和需要将其上升为国家标准；联邦、地方政府的信息系统，以及从事商品、工程、服务等采购活动的法人的相关信息系统在运行期间，不得使用未纳入设备（包括软件）使用目录清单的境外设备和数据库系统等；联邦政府部门、地方自治机构、国有和市属单一企业、国有和市属政机构，与公民/自然人和组织之间进行电子交互时，应确保交互过程符合“信息加密”的相关规定；通信运营商有义务对非法侵犯个人信息权的信息进行处置；拥有独立域名并利用互联网进行信息传播的组织和个人，若发生违反《通信法》规定的行为，应追究其行政、民事或刑事责任。

2.3.2 对信息访问的限制性规定

法案规定，一般情况下，提供接入服务的通信运营商不应公众访问相关信息（包括互联网信息）进行限制，但旨在宣传战争，煽动民族、种族或宗教仇恨和敌意，涉及个人隐私，以及其他刑事或行政规定的信息除外。若访问的信息可能对集中统管产生不良影响，通信运营商应按照《信息、信息技术和信息保护法》有关规定，利用技术手段限

制对上述信息的访问。法案同时还对受限信息的访问进行了规定，如：应按照法律规定、在获得相应机构批准后，方可访问受限信息；当软、硬件工具/设备所有者因依法履行职责需要访问某些受限信息（包括网络信息）时，应向政府主管部门递交纸质或电子版接入申请，相关机构应按规定流程赋予其相应的访问权限。

2.4 主张建立俄罗斯的国家域名系统并启动相关工作

修正案在第二章指出，为了确保俄罗斯联邦境内域名的稳定和安全使用，将建立俄罗斯的国家域名系统，该系统包括一系列相互关联、用于存储和获取相关网址、域名信息的软件和硬件设备。

俄罗斯国家域名系统的申请条件/要求、注册规则/流程（包括其所包含信息的生成）、使用规则（包括获取相关信息的条件和规则/流程）、国家域名清单等由相关政府部门制定，对域名注册的协调工作则交由非营利性机构负责，但联邦政府应介入相关工作。

3 实施前景分析

俄罗斯第 90 号修订案的出台之所以如此引起广泛关注，是因为其相当于俄罗斯在互联网领域应对西方国家（主要是美国）网络霸凌主义的一个公开宣言。目前，针对俄罗斯的网络攻击，特别是有组织的网络攻击日益增多，让俄罗斯在遭受经济损失的同时，还面临着颜色革命和网络恐怖主义的风险，致使俄罗斯当局下决心维护其互联网主权。

3.1 建立独立的互联网体系势在必行

2015 年以来，面对日益复杂的国际形势和网络空间威胁，俄罗斯对其国家战略进行了新一轮的修订。无论是新的《国家安全战略》《军事学说》还是《信息安全战略》，均突出强调“信息空间威胁已成为继传统威胁之后俄罗斯不得不面对的第 4 种威胁”，信息通信技术（包括网络攻击）正越来越多地被用以达成“军事、政治目的”，“信息空间主导权的争夺日渐激烈”。美国作为国际互联网的创建国，拥有着得天独厚的优势（不但拥有主根服务器，还拥有 12 台辅根服务器中的 9 台），掌控着整个互联网。作为美国“天生”假想敌的俄罗斯，不可能长期依赖于被美国操控的国际互联网，

其早在 2015 年就颁布了《关于俄罗斯联邦信息安全若干问题》的 260 号总统令,开始着手构建面向广大政府机构(包括总统办公厅、议会及司法执法等机构)的国家信息通信网^[5]。该网采用安全隧道等防护手段与国际互联网隔离,建立相对独立的互联网体系在俄罗斯看来只是个时间及形式的问题。

3.2 资金将是该法案执行的最大障碍

虽然目前建设独立的互联网体系在俄罗斯国内已达成普遍共识,有关部门还曾于 2019 年 3 月组织过一次“断网”演练,在技术上似乎已无大的障碍,但资金问题将是该法案落实的最大障碍。据法案提出者估算,独立互联网建设大约需 200 亿卢布,这与政府近年用于信息化和数字经济建设所需资金大体吻合(俄罗斯在 2019—2021 年国家预算中已安排 308 亿卢布资金,其中 208 亿卢布将用来采购信息系统),不需要太多额外支出^[6]。但据专家测算,这 200 亿的建设资金并没有考虑到对通信运营商的补偿问题,以及运营企业的设备建设资金,如果全部计入其中,其资金需求总量可能高达 1 340 亿卢布甚至更高^[6]。俄罗斯通信和大众传媒部副部长奥列格·伊万诺夫在接受记者采访时也表示,该法案实施所需资金暂时还无法最终确定。支出不菲也是该法案在推出伊始就招致部分财政金融界人士反对的重要原因之一。

3.3 网络建成后将只是一个备用网络

尽管此法案一经推出就引起国际社会广泛关注,但在全球政治经济包括私人来往日益紧密的今天,建立一个长期与外界隔绝的网络空间并不现实,也不符合俄罗斯的利益需求。该法案的提出,或将可以为俄罗斯政府限制某些群体或地区接入境外网络系统提供技术可能。这一“世外桃源”式的网络空间,用俄罗斯联邦通信、信息技术和大众传播监管总局局长阿列克谢·沙洛夫的话说,“将会‘像核武器’一样处于‘休眠状态’”^[7],俄罗斯建设这样一个网络平台的能力宣誓意义可能更浓一些。俄罗斯这个用以应对紧急情况/状态的“备用信息基础设施”,只有在紧急情况下才会启用,用以将整个国家的网络系统与国际互联网断开。

3.4 新网络的安全性和效果受到质疑

目前,俄国内已将其认识统一到“主权互联网”的建设并不是让俄罗斯人脱离互联网,而是要在紧

急情况下保障国民能够继续使用互联网”的层面,因而该网络平台建设得到了大多数人的支持。但相关网络系统建成后的安全性和有效性仍受到质疑。有专家认为,法案的实施不但会降低俄罗斯网络的运行效率,使其变得更慢、更昂贵,最终导致面向普通消费者和联网设备的通信服务质量下降,从而对智慧城市、交通基础设施相关项目的建设和工业互联网发展产生不利影响,而且还会使俄罗斯现有的信息网络系统变得更加脆弱^[8]。除非俄罗斯拥有相当的技术实力(目前提出的一些技术解决方案的可行性并未得到广泛认可),否则将如此大量的信息通信网络(包括信息系统)集中起来,实施集中统管,将增大安全风险,如遭到黑客攻击、防范措施失效,其结果可能是灾难性的。更有专家指出,实施集中统管后,俄罗斯可能遭受断网威胁的等级将上升至“高等”级别。

综观第 90 号修订案全文,尽管“主权互联网法案”提出的建立俄罗斯国家域名系统、实行路由交换清单制等措施有助于“俄罗斯互联网”的独立与可控,也有助于减少对国际互联网的依赖,俄罗斯有关部门也正在积极贯彻落实相关工作,但受资金、技术等因素的掣肘,要实现真正意义上的“主权互联网”,俄罗斯仍任重道远。■

参考文献:

- [1] Людмила Бокова. Отключить людей от интернета невозможно. Соавтор законопроекта о «суверенном Рунете» объяснила его суть[EB/OL]. (2019-02-09)[2019-05-20]. <https://info24.ru/news/otkljuchit-ljudej-ot-interneta-nevozmozžno-soavtor-zakonoproekta-osuverennom-runete-obyasnila-ego-sut.html>.
- [2] Виталий Алексеев, Карашаш Ногаева. Это и есть shit, пусть и не золотой. Как 20 млрд на борьбу с Дуровым превратились в деньги на создание суверенного Рунета[EB/OL]. (2019-02-13)[2019-03-12]. https://m.dp.ru/a/2019/02/13/JEto_i_est_shit_pust_i.
- [3] Президент Правительства Российской Федерации Путин. Федеральный закон от 01.05.2019 N 90-ФЗ "О внесении изменений в Федеральный закон "О связи" и Федеральный закон "Об информации, информационных технологиях и о защите

- информации"[EB/OL]. (2019-05-01)[2019-05-02]. http://www.consultant.ru/document/cons_doc_LAW_323815/.
- [4] Президент Правительства Российской Федерации Путин. Федеральный закон "О связи" от 07.07.2003 N 126-ФЗ[EB/OL]. (2003-06-18)[2019-05-12]. http://www.consultant.ru/document/cons_doc_LAW_43224/.
- [5] Президент Правительства Российской Федерации Путин. Указ Президента РФ от 22.05.2015 N 260 "О некоторых вопросах информационной безопасности Российской Федерации"[EB/OL]. (2015-05-22)[2019-05-18]. http://www.consultant.ru/document/cons_doc_LAW_179963/942772dce30cfa36b671bcf19ca928e4d698a928/.
- [6] Наталья Корченкова. С суверенностью в завтрашнем дне:Эксперты при правительстве оценили затраты на автономный рунет[EB/OL]. (2018-12-25) [2019-05-18]. <https://www.kommersant.ru/doc/3842329>.
- [7] Александр Жаров. Глава Роскомнадзора сравнил закон о суверенном Рунете с ядерным оружием[EB/OL]. (2019-04-16) [2019-05-12]. <https://www.rbc.ru/rbcfreenews/5cb5cbdb9a79472b02d33996>.
- [8] Денис Вышинский. Операторы задумались о вещном. Суверенный рунет может оказаться слишком медленным для IoT[EB/OL]. (2019-03-21)[2019-05-22]. <https://www.kommersant.ru/doc/3917500>.

Analysis of the Main Contents and Implementation Prospect of Russia's "Sovereign Internet Act"

YOU Xian-ju, XIE Jing, GANG Xin-xin

(China Industrial Control Systems Cyber Emergency Response Team, Beijing 100040)

Abstract: Russia's "Sovereign Internet Act" has drawn international attention for its advocacy of an independent Internet system. In order to fully understand and grasp the thinking and implementing path of the construction of the independent Internet system, on the basis of a large number of relevantly collected and sorted materials, combined with years of accumulation, the paper comprehensively introduces the legislation background, as well as the related content, and then carry on the forecast analysis to its future implementation prospect, so as to provide reference for the relevant departments of China to carry out network construction.

Key words: Russia; independent internet; sovereign internet act