互联网恶意软件的行政法治理

王小龙
(浙江省通信管理局 政策法规处,浙江 杭州 310000)

[摘 要] 互联网恶意软件因其强制安装、难以卸载、恶意捆绑、恶意收集用户信息等行为侵犯了用户隐私权、知情权、互联网信息市场秩序及公共安全秩序。目前中国对恶意软件的治理呈现出刑事在前、行政规制落后的情况。而结合恶意软件阶段性、复杂性的特征及中国的互联网管理体制,应当充分发挥行政法律规范的评价、指引、强制作用,通过梳理法律法规规定,完善法律依据,提高联合执法效率、建立多方位全方面的综合治理体系实现对恶意软件问题的有效治理。

[关键词] 互联网;恶意软件;互联网信息服务;行政规制
[中图分类号]D912.1 [文献标识码] A [文章编号]1671-6973(2017)04-0042-07

应用软件作为互联网产业的重要组成部分,对我国信息经济的发展起着无可替代的作用,而且随着科技的发展及提速降费政策的纵深推进,应用软件还将进一步覆盖到生活的各个方面。相应的,恶意软件作为应用软件的一种形式也正搭着软件服务生活的春风入侵到千家万户。与其他软件相比,恶意软件带来的不是服务,而是侵害。所谓的恶意,既指客观上的恶,即软件的功能设计存在妨碍他人权益的情况;也指主观上的恶,即其作为产品,受到不同主体、不同方式、不同目的影响,进而产生了法律上"恶"的后果。目前学术界对恶意软件的研究主要是集中在网络侵权、网络犯罪、网络安全技术保障等方面,所研究的是主观上的恶,相应的治理路径是民事裁决与刑事追责。然而从恶意软件日益严重的危害性、复杂性及责任追究体系的构建角度看,对行政权力的忽视可能是恶意软件仍然无法根除的重要原因。

一、恶意软件的界定

2006年中国互联网协会发布了《抵制恶意软件自律公约》,较早对恶意软件的定义进行了概括。"恶意软件也被称作流氓软件、间谍软件、广告软件,是指在未明确提示用户或未经用户许可的情况下,在用户计算机或者其他终端上安装运行,侵害用户合法权益的软件,但不包含中国法律法规规定的计算机病毒。"其特征表现为:强制安装、难以卸载、浏览器劫持、广告弹出、恶意收集用户信息、恶意卸载、恶意捆绑以及其他侵犯用户知情权和选择权的恶意行为。只要符合其中一项即可称之为恶意软件。

有人根据恶意软件的形式将其分为六个种类[1]:

1.广告软件(Adware)。广告软件是指未经用户允许,下载并安装在用户电脑上,或与其他软件捆绑,通过弹出式广告等形式牟取商业利益的程序。

2.间谍软件(Spyware)。间谍软件是一种能够在用户不知情的情况下,在其电脑上安装后门、收集用户信息的软件。

3.测览器劫持。浏览器劫持是一种恶意程序,通过浏览器插件、BHO(浏览器辅助对象)、Winsock LSP等形式对用户的浏览器进行篡改,使用户的浏览器配置不正常,被强行引导到商业网站。

4.行为记录软件(Track Ware)。行为记录软件是指未经用户许可,窃取并分析用户隐私数据,记录用户电脑使用习惯、网络浏览习惯等个人行为的软件。

[收稿日期] 2017-02-10
[作者简介] 王小龙(1989-),男,河南邓州人,中国社会科学院研究生院宪法学与行政法学硕士,主要研究方向为行政法学、信息法学。

5.恶意共享软件(malicious shareware)。恶意共享软件是指某些共享软件为了获取利益,采用诱骗手段、试用陷阱等方式强迫用户注册,或在软件体内拥绑各类恶意插件,未经允许即将其安装到用户机器里。

6.其他。随着网络的发展,恶意软件的分类也越来越细,一些新种类的恶意软件在不断出现,分类标准必然会随之调整。

上述概念是行业协会从技术功能的角度进行的总结,但在我国法律规范中,并没有采用恶意软件的概念,只有恶意程序的规定。即便是最新颁布的《网络安全法》也仍然沿用了行业规范性文件中"恶意程序"的名称,而且并没有给出定义。因此,对恶意程序的定义可以参照现有规范性文件的阐释——即采用《移动互联网恶意程序检测与处置机制》中对移动互联网恶意程序的界定。在该文件中,移动互联网恶意程序是指运行于包括智能手机在内的具有移动通信功能的移动终端之上,存在窃听用户通话、窃取用户信息、破坏用户数据、擅自使用付费业务、发送垃圾信息、推送广告或欺诈信息、影响移动终端运行、危害互联网网络安全等恶意行为的计算机程序。

结合行业协会及规范性文件对恶意程序的定义,可以发现恶意软件与恶意程序在性质、表现特征、危害后果等方面是重合的。因此,本文认为恶意软件是指"运行在各类终端上,存在窃听用户通话、窃取用户信息、破坏用户数据、擅自使用付费业务、发送垃圾信息、推送广告或欺诈信息、影响移动终端运行、危害互联网网络安全等恶意行为的计算机程序"。

二、恶意软件治理的紧迫性

(一)互联网应用软件产业稳健发展的需要

根据中国互联网络信息中心《中国互联网络发展状况统计报告(2016年7月)》的统计,截止2016年6月,中国网民规模达7.10亿,手机网民规模达6.56亿。手机上网使用率为92.5%,台式电脑和笔记本电脑接入率分别为64.6%和38.5%;平板电脑上网使用率为30.6%,手机上网主导地位得到进一步强化。与此同时,作为上网主要产品的互联网应用软件用户规模均呈上升趋势。即时通信、搜索引擎、网络新闻、网络视频、网络音乐、网上支付、网络购物等应用用户规模均已超过4亿。互联网应用软件已经随着互联网络设施水平的进一步提高和网民数量的提升,日益渗透到网民生活的方方面面。

在应用软件如火如荼地发展形势下,恶意软件一方面通过捆绑合法商业软件(共享软件)的形式造成用户感知度、体验度下降,通过植入同业竞争者的网站或者平台,成为互联网市场不正当竞争的武器;另一方面通过强制安装、手机用户信息、弹窗广告等方式消耗用户资源系统,降低用户终端安全系数,成为黑客、木马僵尸、病毒等入侵的对象,非常不利于互联网应用软件市场的健康发展。

(二)以恶意软件为核心形成了庞大的灰色产业链

根据国内知名杀毒软件瑞星公司的公告,恶意软件的发展经历了四个阶段:(1)恶意网页代码时代(2001年—2002年)。该阶段主要通过在网站中植入恶意代码的形式修改用户的IE浏览器主页,提高网站访问量。(2)插件时代(2003年—2005年)。该阶段因2003年"中文上网"解析域名软件的出现,引发一大批同质化插件程序泛滥网络,影响网民的上网体验。(3)软件捆绑时代(2005年—2006年)。因反恶意软件的工具开始广泛应用,依赖网站设置方式受到限制,一些厂商开始通过与共享软件捆绑的方式,向用户的电脑中安装恶意软件,并支付一定费用。(4)流氓软件病毒化时代(2006年下半年至今),在共享软件捆绑的形式被公众和用户指责后,编写和传播病毒华成为恶意软件的特点。

恶意软件表现形式的变化离不开巨大灰色产业链的推动,灰色产业链的形式分为两类:一类是恶意软件的开发者、经营者与共享软件或者下载商店以协议的方式达成捆绑交易后,向下游具有大量投放广告需求的广告主提供弹窗流量或者捆绑其他插件。一类是恶意软件的开发者、经营者未经他人同意,以网页链接、钓鱼网站、假冒软件或者捆绑合法软件等形式,强制安装进用户电脑,一方面以获取他人信息为目的在网上进行贩卖或进行诈骗、骚扰等违法犯罪活动,一方面向广告主兜售流量资源。产业链的结构在2011年工信部《规范互联网信息服务市场秩序若干规定》(以下简称"规定")出台后发生了较大改变,由原来的共享软件捆绑搭售,转变为恶意软件单独运作与捆绑搭售并存的局面。随着移动终端和网民数量的大幅增加,个人信息的珍贵程度进一步凸显,以获取用户个人信息为目的的恶意软件产业链成为主流。

(三)恶意软件产业的法律治理效果不够明显

自1991年互联网全面商业化以后,互联网应用的发展速度远远超过了互联网技术的发展(完

善)程度。但与此同时,互联网安全问题也随之而来。“在没有更加是成熟的网络软硬件架构、网络编程语言出来的时候,只能在现有的不甚完善的网络基础上修修补补,结果造成互联网上的安全漏洞百出。”[2]一方面互联网自身分布式的扩散、虚拟空间的特点从一诞生就存在着安全漏洞,这是无可避免的。但另一方面却是人为的滥用造成了恶意软件的泛滥。恶意软件的治理一直是法律治理的难题。立法层面,法律法规的滞后面对一日千里的互联网发展形势表现得淋漓尽致。2001 年制定的《计算机软件保护条例》到 2013 年修改间隔了十多年,2000 年出台的《互联网信息服务管理办法》沿用至今,《网络安全法》直到 2016 年才迟迟出来。

目前,我国对恶意软件的规定主要体现在《规范互联网信息服务市场秩序若干规定》,该规章出台的背景为 2011 年的“3Q 大战”,其目的主要是解决互联网信息服务提供商之间的不正当竞争,但在内容上延伸到了对所有互联网软件使用的规范。然而随着恶意软件的形式逐渐转变为单独运作与捆绑共享兼存的模式,原有的互联网信息服务秩序再次陷入无法可依的情形。此外,在执法层面,中国互联网执法体制实行的是内容和渠道分治的管理模式,推诿扯皮、相互制约的情形屡见不鲜,对恶意软件的治理更加侧重于通过预警、查处等方式实现,可以说,恶意软件的治理从立法到执法,均缺乏统一的逻辑及规范的体系。

三、恶意软件侵犯的权利需要行政法调整

行政管理法律关系是行政法律规范的主要调整对象,作为行政权力的承载主体,行政机关根据法律法规的授权行使调整社会主义市场经济秩序的权力。恶意软件引发的后果既是对网络用户的隐私权、财产所有权、知情权、选择权等权利的侵犯,也是对互联网信息服务市场的扰乱,甚至威胁到了国家的安全和社会的稳定。

(一)恶意软件对网络用户民事权益的侵犯

网络时代的到来引发了许多新型社会问题,但是无论科技如何发达,计算机的服务对象始终是人类。因此,“在现实社会中有关民事主体基本民事权利的制度设计同样也应该在网络环境中得到适用。”[3]网络用户作为互联网的使用者,是恶意软件直接侵害的对象。在互联网时代,个人信息是一种无形的宝贵财产,也是网络内容提供者和广告主最为需要的资源。恶意软件通过在用户电脑安装插件的方式,未经用户同意,获取用户的姓名、身份证号、联系方式、家庭住址、账号账户等个人信息,通过贩卖、兜售等方式售于广告主、大众商家等需求方,使得个人饱受广告邮件、电话、短信等骚扰之苦,是对用户个人隐私的窥探和泄露,严重侵犯了个人隐私权。用户的个人信息,特别是支付宝、银行卡等财产信息泄漏后,很容易被不法分子利用,修改或者移除,进而成为窃取用户个人财产的渠道。安装的恶意软件无法卸载,侵占用户终端内存,影响用户正常使用,擅自删改用户程序,是对用户财产处分权的限制。

网络用户访问网站、获取信息服务时,恶意程序在未告知并经消费者同意的情形下即下载到用户浏览器,弹出广告或被修改了 IE,显然侵犯了用户的知情权。从另一个角度,恶意软件在安装到用户终端前,“未向用户明示不能正常被删除、影响其他软件正常使用等情形,不同程度地构成了对消费者的欺诈。”[4]

(二)恶意软件不利于构建规范的互联网信息服务市场秩序

恶意软件的影响不仅限于个人,对其他互联网信息服务提供者及互联网信息市场都产生了恶劣影响。“3Q 大战”正是这样一个特例。还有商户通过恶意软件假冒他人网站,或者链接至自身网站,混淆用户,抢夺资源。还有商户在其他竞争者网页或者软件中装入恶意软件,以弹窗广告、恶意下载、DDoS 攻击等形式造成用户恶性体验,进而影响到其他竞争者的网民流量和商业利益,“明显违反了善良风俗、商业道德和城市信用原则,扰乱了信息服务市场经济秩序,属于不正当竞争行为。”[5]

(三)恶意软件对互联网安全的影响

长期以来,互联网安全一直是互联网技术发展的重心,也事关人们对互联网的看法与态度,更是互联网立法的重要领域。纵观中国互联网近二十年的发展,关于互联网安全的立法一直走在前列,但关于恶意软件的立法却因为其看似更具民事色彩而乏善可陈,实则恶意软件的影响并非仅限于普罗大众,还威胁着互联网的安全。互联网安全本质上是互联网信息安全,凡涉及到互联网上信息的保密性、完整性、可用性、真实性和可控性的相关技术都属于互联网安全的范畴。恶意软件通过自动下载,植入程序,主动实施窃听(非法访问数据、获取密码文件)、欺骗(恶意代码、获取口令)、拒绝服务等方式对互联网信息进行搜集,加工,并辅助其他人工手段,形成庞大的互联网络诈骗团伙或者犯罪

群体对个人、企业，甚至国家机关实施网络攻击，导致大量个人信息、秘密信息遭到泄露，破坏了原有终端中个人和组织设置的安全软件性能，侵害了用户对信息私密性的目的，严重影响了互联网的稳定健康发展，甚至对社会稳定、国家安全都造成了极为严重的损失。

（四）恶意软件需要行政法的调整

互联网在中国的发展只有二十多年的历史，但带来的经济效益和社会影响却是巨大的。这样一种反差反映出互联网与经济社会生活的紧密结合度已经到了如胶似漆的状态。但正是这样的状态为互联网的立法带来了难题。法律作为调整社会关系的一种手段，一方面要为互联网经济的发展保驾护航，一方面要加强对互联网衍生问题的规范。互联网的发展与安全是相辅相成的，但在互联网技术、市场都尚未成熟的情形下，二者的问题就愈发突出。在这样的情况下，摸着石头过河无疑是政府最为惯常的做法，但也最容易出现“头疼医头，脚痛医脚”的情形，即不完善的法律规范无法实现完善的法律效果。应用软件作为近两年发展迅猛的互联网产品对社会民众的生活影响尤为巨大，吃穿住行钱已经离不开应用软件的使用。应用软件自身并不存在的法律上的问题，只存在技术安全的风险。恶意软件本质也是应用软件的一种，但因为目的、手段、结果的不正当性被认定为“恶意”。由此可见，治理恶意软件及其他互联网产品的核心问题即是该软件是否引发了相应的法律关系。

在目前发生的恶意软件的案件中，将网民与恶意软件制造者开发者之间的关系确认为侵权的是比较多的，也是符合保护公民隐私权、知情权等权益所要保护的客体的，而且从权利救济的角度考虑，对公民也是有利的。在刑法规制方面，刑法修正案七增设的“非法获取计算机信息系统罪”、“非法控制计算机信息系统罪”、“提供用于侵入、非法控制计算机信息系统程序、工具罪”等罪名，刑法修正案九增加的个人信息、网络传播非法信息等条文对恶意软件引发的后果所需要承担的刑事责任有了非常明确的规定。写入刑法，可以极大地增加违法犯罪的成本，对利用恶意软件实施违法犯罪行为的不法分子进行震慑，这些都为治理恶意软件提供了很好的治理依据。但从目前国家的互联网治理体系来看，行政机关是应当在恶意软件的治理中占据重要地位的。

首先，从中国的互联网法律体系可以看出，行政管理法律体系框架已经基本形成，且涉及到互联网许可、管理（竞争、安全）、设施建设、安全、知识产权等各个方面，法律、行政法规、部门规章、规范性文件等不同层级效力的法律依据也已逐渐完备，为更好的解决协调互联网的发展及治理问题提供了较为完备的法律依据。其次，恶意软件作为一种不断变化的技术应用，与其相随的违法类型也处在不断变化中，如不能及时对相应的行为作出认定，从时效上则会失去先机，既增加了主管部门的履职风险，更不利于保护个人和组织的合法利益。最后，在法律法规尚未有明确的情形下，通过行政手段或者发布规范性文件等途径及时对恶意软件案件做出回应，把握处理恶意软件问题的主动权，进而上升到立法高度，实现对恶意软件背后所形成的灰色产业链进行更为全面的规制是比较可行，也是更为有效的。然而，在目前的法律规范体系中，对恶意软件产业链的治理却是刑事规制走在前列，行政法律走在后头，除了互联网多头管理等原因外，也摆脱不了行政不作为的嫌疑。

总之，不论是从职权法定的角度，还是从解决恶意软件产业链根源问题的角度，亦或是从保护公民和组织财产的角度，都必须发挥行政法律规范的指引、预测、评价和强制的作用，以切实履行为民监管、依法执政的承诺。

四、恶意软件治理中存在的问题

（一）《网络安全法》的意义及缺陷

2016年《网络安全法》的颁布对整个互联网的治理具有极为关键的作用，在恶意软件的治理上也体现的尤为明显。根据该法第二十二条的规定，网络产品、服务的提供者不得设置恶意程序。第四十八条，任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。该法意图从“设置”行为出发，对可能的主体“网络产品、服务的提供者”和“任何个人和组织”进行规范，并规定了相应的处罚措施，弥补了立法中法律依据中对恶意软件治理的空缺。

但该法却也存在比较突出的缺陷：一是未对恶意程序进行明确定义。根据目前可以查询到的文件，只有工业和信息化部在《移动互联网恶意程序监测与处置机制》中对“移动互联网恶意程序”作了明确规定。虽然二者具有一定的借鉴意义，但“尽管法律语言的模糊边界既确定无疑又必不可少，但这并不意味着立法者可以顺理成章地对法律语言中的模糊性采取习以为常的态度”。[6] 从立法的科学性及操作性看，“恶意程序”定义不清，可能导致

自由裁量权的滥用。二是在处罚条款中，使用了“有关主管部门”的概念。作为一部基本法，基于机构变更等情形，使用概念性的名词去表达本无可厚非。但作为对行政处罚主体的规定显然有些不够准确，而这个问题恰恰是期望得到解决的。三是该法并未就不同政府部门的职责作出较为明确的规定。

（二）立法体系不够健全

《网络安全法》的出台在顶层制度的设计上已经得到弥补，但体系的完整性仍然有待建设。我国对恶意软件的治理依据主要以规范性文件、部门文件为主，如《工业和信息化部、公安部、工商总局关于打击治理移动互联网恶意程序专项行动工作方案的通知》（工信部联保[2014]153号）、《工业和信息化部关于加强电信和互联网行业网络安全工作的指导意见》（工信部保[2014]368号）、《移动互联网恶意程序监测与处置机制》（2011年）等，部门规章中只有工业和信息化部《规范互联网信息服务市场秩序若干规定》从互联网信息服务市场秩序的角度对利用软件实施恶意行为的认定及惩处作出了规定，其他相关的行政法规、部门规章主要从技术安全、信息安全、互联网等侧面角度对恶意软件作出回应。如2000年出台的《电信条例》（2016年修改）对电信业务经营者不得限制用户接受服务、利用电信网从事窃取或者破坏他人信息、损害他人合法权益的行为作出了明确；公安部2005年出台的《互联网安全技术保护措施规定》规定了互联网信息服务提供者、联网单位对其提供的安全技术保护义务。工商管理部门作为负责软件销售等市场行为的主管部门，除了联合发文外，很少利用行政立法的手段去规制。如前所述，恶意软件作为应用软件的负面产物，其存在已经极大地侵犯了网民的合法权益，无论在影响范围，还是影响深度上都已经成为去之不掉的顽疾，而随着互联网络的进一步普及和应用软件的全面覆盖，恶意软件的问题只会越来越突出。因此，必须尽早将恶意软件问题纳入到行政立法中，在立法层面处置有据。

（三）执法力量薄弱，职责分工不清

中国对互联网实行的是渠道和内容分开治理的模式，即内容认定部门及互联网网络治理部门非同一机构。互联网案件的处理由各部门根据法律法规和职责分工分步处理，内容认定部门作出法律事实判断，并给予相应处罚，再由互联网主管部门实施关闭网站等结束行政处罚行为。在恶意软件的治理中，发挥主要作用的有主管互联网的通信管理部门、查处违法犯罪行为的公安机关以及负责软件流通、保护消费者权益的工商管理部门。相对于其他部门，通信管理部门虽然是互联网络的主管部门，但在执法力量上是远远落后的。一是编制急缺。各省市通信管理部门只有二十多人的编制。二是在地市没有相应的分支机构，应对数量庞大的互联网络案件难以为继，这也是目前的互联网管理以监测、技术处置为主的主要原因。此外，执法力量的匮乏也为互联网络的事中事后监管带来了难题。恶意软件通常需要寄生于其他的网络服务提供者，作为发证机关，通信管理部门应当对网络服务提供者的经营行为及时进行监督检查，但事实上，受制于人员的力量，其主要通过网络协调机构或者其他监测机构的报告来进行监督，监督检查的效果自然可以预见。公安部门和工商管理部门自身都拥有强大的执法力量，但其对恶意软件的管理是特定的，主要从“九不准”信息的认定及网络技术安全体系、刑事犯罪的角度进行管理，对关联主体（互联网内容服务提供者）未能尽到完全的管理义务（断开接入、关闭网站等）；工商管理部门主要对非法软件的销售、买卖及侵害消费者权益保护等方面进行履职，但《消费者权益保护法》关于消费者与经营者的消费法律关系能否适用于恶意软件的法律关系在法理上还值得探讨。[7]反不正竞争法虽然可以适应，但大多内容已经在《规定》中得以体现，作为主管机关在管辖权上存在交叉管理的尴尬。三家主管部门不仅在执法上面临着相应的问题，在联合执法的过程中也存在着未按照规定及时移送案件、踢皮球、移送文书不规范、执法配合程度较低、查办案件阶段性特征突出等问题。

五、治理恶意软件的行政法思考

（一）完善恶意软件治理立法体系

1.以保护公民和其他组织权益和互联网安全为核心，明确恶意软件的法律概念。立法是否明确、科学直接影响执法效果和司法认定，因此应当遵循科学、合理、合法的原则对恶意软件的概念进行界定。具体而言，可以从主观、客观、表现形式（特征）等方面进行尝试。客观上，恶意软件是互联网技术应用而成的虚拟产品，是应用程序的一种表现形式；在传播的过程中，客观上侵犯了他人的人身权、财产权或者社会秩序、公共利益，具有一定的危害性；主观上鉴于恶意软件来源的难以确定，如果按照侵权关系的要求符合主观故意，则难免会与公平原则相冲突，因此建议在认定时，不论主观故意或过失，只要产生了客观后果，即可认定为恶意。

在表现形式方面，主要以是否违背当事人意愿为标准对恶意软件的特征进行概括，即发生了强制、劫持、弹出等当事人不能掌控的行为。

2.完善现有法律规范。《网络安全法》作为基本法具有高度的概括性，其具体条文的落实还需要相应行政法规和部门规章进一步细化，提高可操作性。建议对《电信条例》《规范互联网信息服务市场秩序若干规定》等部门规章进行修改，明确引入恶意软件的概念，吸收现有条款对恶意程序的规范内容。在罚款额度上按照《网络安全法》规定的处罚种类和幅度进行调整，以照顾条文的一致性。

3.增加各部门之间的处罚程序衔接条款或者建立相应的制度。在国内分头并治的互联网管理体制下，对同一互联网违法行为的处罚是由两个部门共同作出的，但在目前与恶意软件行为相关的处罚条文中，并不存在连续性处罚行为的规定。这对追究恶意软件从制作、传播到侵害相对人的权益的全过程各个主体的责任是不利的，建议在相关涉及互联网络的规定中，增加相关部门的责任衔接条款。

4.改变以协调为主、处理为辅的理念，强调标本兼治。目前我国对恶意软件持预防监测的治理理念，处理手段主要是屏蔽、删除、防护等，不能够对恶意软件的制作者、传播者构成强有力的震慑；再者，行政管理部门也缺乏主观上的重视，没有严格按照联合执法文件的要求进行案件移送查处等程序，因此需要改变观念，增强认识，加大考核力度。

（二）优化行政资源配置，完善联合执法机制

1.合理配置执法资源。尽管庞大复杂的政府机构一直为人诟病，但应当看到的是，随着经济社会发展趋势的改变，传统的执法资源分配已经不符合现实社会的需求，互联网产业的崛起及全面渗透使互联网行业主管部门执法力量薄弱的问题逐渐暴露出来。但在国家严格控制编制数量、精简政府部门的理念及形势下，期待通过增加行政编制填补执法力量的路径已经被切断。因此，可以考虑发挥行政授权和行政委托的作用，如授予其下属的事业单位或者行业协会一部分管理职责，通过下放职权的方式，还权于民，既发挥相关网络安全管控平台的技术优势，也可以调动企业参与社会管理的热情。

2.以权力清单和责任清单的方式明确不同机构治理恶意软件的职权范围，解决管辖问题。自2015年中办、国办印发了《关于推行地方各级政府工作部门权力清单制度的指导意见》后，“两单”成为厘清政府职能、规范政府权力的主要抓手。其最大优势在于，通过明确不同政府部门的法定职责，划清各自的管辖权限，力破权责不清、踢皮球的难题。结合目前存在的问题，两单关注的重点应集中在网信办和信息通信管理机构关于互联网的审批权以及其他政府部门与信息通信管理部门、网信部门之间内容管理的职权划分问题。

3.参照综合执法管理机构成立专门的联合执法队伍，形成常态化的互联网恶意软件治理机制。恶意软件在传播范围、传播方式、追查难度方面都要超出其他案件，更具有隐蔽性和反侦察性，如果不能及时应对、快速处理，则此类案件会随着时间的变化而更加复杂。通过建立联合执法机制，整合执法力量，可以充分利用关联政府部门的行政资源，合理均摊执法力量，弥补一家执法难度大、人员不足的缺陷。

（三）形成全方位的恶意软件治理体系

互联网的治理是一项庞大而复杂的社会工程，特别是在互联网与其他产业结合日益紧密的情势下，单纯依靠行政机关的力量不能满足实际需要，还需发挥更多社会群体的力量。

一方面，恶意软件的传播载体具有特定性，即主要是通过触发链接引起。而恶意软件的链接大多是通过QQ、微信群、网页、博客等途径进行传播，因此作为QQ、网页等载体的管理者就应当担负一定的责任，加强网络信息的审核、完善安全防护体系、建立举报快速处理机制、留存相关日志信息等。

另一方面，作为恶意软件的主要传播源——应用商店，应当严格按照《移动互联网应用商店网络安全责任指南》的要求履行相应的义务。大力推行软件注册实名制，加强对发布软件内容的测验、审核；完善事前审查、事中监督、事后删除保存的机制，编制应用软件的安全防护网。

此外，应当发挥行业协会、主要互联网安全企业的作用。互联网协会、国家互联网络安全管理中心、互联网举报处理中心等机构为恶意软件的治理提供了良好的技术支撑和反馈平台，应当完善此类机构和相关主管部门之间的案件处理机制，形成平台接受——行政机关处理——平台处理的模式；充分发挥行业组织的自律作用，搭建恶意软件黑名单，对相关企业或者个人列入失信名单，并及时对各类恶意软件数据或者事件进行通报，提高社会公众的防范意识。

最后，普通网民也要提高应用软件的使用防范

意识，通过官网、权威平台等下载使用软件，提高维权意识，及时通过各种途径举报、投诉不良违法行为。

六、结语

恶意软件的问题暴露出我国互联网治理的背后缺乏对人本利益的重视。中国原有的互联网治理一直是以维护互联网安全为中心，但恶意软件的出现却给这一思维带来了挑战，让普通公民开始意识到互联网所带来的对个人权益的威胁已经并不遥远，可能就在自己身边。近几年，中国已经通过加强立法、加大执法力度等途径对恶意软件进行打击和清理，但传统的监管思维已经不能适用互联网时代的需求。“如果法律界依旧习惯性地用传统的制度和学说框架去应对新现象，不仅无法对社会现实提出有说服力的解释，还可能阻碍互联网这一新兴产业的健康发展”。[8] 如何转变思路，从立法层面，从保护人权方面出发去建立一套完备的互联网治理体系，不仅是应对恶意软件问题的需求，也是构建法治、和谐的互联网秩序需要研究的重大课题。

[参 考 文 献]

[1] 燕红文. 中国流氓软件治理困境中的若干问题研究[D]. 山西：山西大学，2008：8.

[2] 凤建军. 流氓软件法律问题研究[J]. 河北法学，2008(6)：25.

[3] 王新华、张莎. 恶意软件侵权的法律思考[J]. 江西社会科学，2008(7)：207.

[4] 赵衍. 互联网时代的信息安全威胁：个人、组织和社会[M]. 北京：企业管理出版社，2013：14.

[5] 郑淑蓉.“恶意软件”的危害及其治理[J]. 生产力研究，2009(2)：61.

[6] 冯玉军. 新《立法法》条文精释与适用指引[M]. 北京：法律出版社，2015：26.

[7] 凤建军. 流氓软件法律问题研究[J]. 河北法学，2008(6)：25.

[8] 王利明. 论互联网立法的重点[J]. 法律科学，2016(5)：110.

（责任编辑：闫卫平）

The Administrative Law Governance of Internet Malware

WANG Xiao-long

(Zhejiang Communications Administration, Policy And Regulation Department, Hangzhou 310000, China)

Abstract: Internet malware violates the right of privacy, the right to know, the order of the Internet information market and the order of public security due to its mandatory installation, difficult to uninstall, malicious bundling, malicious collection of user information and other acts. At present, the management of malicious software in China presents the situation that the administrative regulation lags behind the criminal. And combined with the internet management system and the characteristics of malicious software, that is periodicity and complexity, we should give full play to the role of evaluation, guidance and enforcement of administrative legal norms and achieve the effective governance of malicious software through carding laws and regulations, improving legal basis and the efficiency of joint law enforcement and establishing a comprehensive system of management in a directions.

Key words: Internet; Malware; Internet Information Service; Administrative Management