信息安全法研究

CYBERSECURITY LAW STUDIES

马民虎　主编

陕西人民出版社

信息安全法研究

主摇编摇马民虎摇摇摇摇
副主编摇李摇岩摇武向阳

陕西人民出版社

顾　问

王渝次摇国务院信息化领导办公室司长

李摇昭摇公安部公共信息网络监察局局长

秦摇海摇国务院信息化领导办公室副司长

吕诚召　国务院信息化领导办公室副司长

郑静清　国务院信息化领导办公室副司长

郭摇明　陕西省公安厅副厅长

雷建平　宝鸡市公安局局长

前摇言

在改革开放的当代中国,信息安全法已经成为法学界和立法机关的研究热点。自员怨怨源年我国颁布《中华人民共和国计算机信息系统安全保护条例》以来,我国在信息安全领域的法制建设工作取得了令人瞩目的成绩。现有的法律法规对保障我国信息化事业的健康发展起到了积极的作用。

但是,随着信息技术的发展和网络在我国社会经济中的广泛应用,我国信息安全立法滞后和不完善的问题也日益突出,其主要表现在以下几个方面:

员、理论研究滞后,立法缺乏总体思路:(员)缺乏系统思路和总体指导原则,立法重复,资源浪费;(圆)内容上声明性条款过多,程序上缺乏可操作性;(猿)对技术发展趋势估计不足,相关领域存在法律漏洞。

圆、队识不统一,监管不力:(员)行业监管与安全监管范围交叉,责任不明;(圆)相关领域多头管理,利益冲突,缺乏协调;(猿)部分法规不符合国情,立法、执法不统一。

猿、重管理、轻保护,公权益与私权益对比失衡:(员)对国家安全和个人、法人利益的包容性缺乏足够认识;(圆)忽视社会力量、市场机制维护信息安全的合理性;(猿)行政法、刑法范围关注较多,民商法领域重视不够。

[illegible]重视防范性的处罚措施，轻视促进发展的法律规范；[illegible]相关法律法规之间缺乏协调，未能给发展留下空间；[illegible]重视市场准入环节的控制，忽视市场退出制度建设；[illegible]信息权属法制不健全，安全信息共享法制建设严重缺位。

受国务院信息办的委托，我组织国内部分信息安全法律专家，针对上述问题进行了系统的理论研究，本书即是该项研究的最终成果。

第一章从概念的“安全观”分析了法的调整范围。

在立法文献中，计算机安全、信息安全、网络安全和网络与信息安全都涉及信息系统安全，但不同的立法背景决定了安全观内容上的差异，也影响了法律所要调整的范围。

“网络”在中文中有多种用法，如电力网络、交通网络、环境检测网络、信息网络、广电网络、电信网络等。从有关信息的网络应用角度，有互联网、局域网络、行业专用网络等。可见，中文中“网络”的使用范围非常广泛。

“网络”在英文中大致有[illegible]和[illegible]两种说法。一般用法是：[illegible]和[illegible]事实上，[illegible]的含义并不仅仅限于计算机系统互联互通，还包括数据存储、处理和运算的各种系统。

[illegible]其本意与计算机相关，[illegible]为计算机空间。因此，称[illegible]为网络空间并不准确。但国内媒体普遍误称之为“网络空间”，因此我们的研究也沿用这一用法。

[illegible]最早出现于[illegible]年美国作家威廉·吉伯森([illegible])的科幻小说“矩阵三部曲([illegible])”，又称“漫生三部曲([illegible])”之一的《神经漫游者》([illegible])。美国《网络空间安全国家战略》指出，[illegible]

是确保国家关键基础设施正常运转的“神经系统”,是国家的控制系统。

[illegible]即[illegible]我们可以理解[illegible]那[illegible]是为确保企业交易、政府运行和国家防御三方面职能所依赖和互联的关键信息基础设施网络的安全。

[illegible]的含义,国内学界认识向来有争议。“中共中央办公厅、国务院办公厅转发《国家信息化领导小组关于加强信息安全保障的工作的意见》的通知”,似乎平息了这一本来能够讲清楚的概念。但国家信息安全战略的研究又掀起了国内对此问题的不小的风波。结合全国人大《关于维护互联网安全的决定》对互联网、网络、信息系统、信息之间关系的“大团圆”总结,似乎对这个问题国人真的纠缠不清了。

实际上,网络安全与信息安全的不同观点,反映着主张者之间的不同利益关系。如果人们真的能够基于国家整体利益考虑,以国民经济与社会对网络空间安全的“依赖程度”作为分析问题的出发点,解决这个困扰我们多年难题的“密钥”似乎并不这么麻烦。

在计算机网络技术的应用初期,信息系统相对独立,还没有成为重要的基础设施。计算机安全或者信息系统安全的核心是“财产安全”,而以机房为中心的信息系统安全概念成为人们关注的焦点,形成了当时被动保护式的安全观。因此,财产权和隐私权、国家利益各自特有的保护方式决定了该时期法的目的定位,“未经授权”则是该时期法的基本规范模式。

随着网络信息技术的迅猛发展,信息系统发展成为国家关键基础设施网络,“病毒”成了人类社会的一种新型“公害”,网络恐怖活动严重威胁着人类社会的安全,信息安全与国家安全、

社会公共安全的关系变得愈加密切。为适应网络信息安全保障的要求,网络信息安全法要十分关注信息安全与应用领域政策的统筹考虑。这在法律规范上的表现就是加强信息监控,强调信息安全策略的规划,关注信息安全风险责任有效控制原则的落实。

随着人类社会对网络空间的高度依赖,网络空间与物理空间相互依存。保障网络信息安全需要政府和全民的共同参与,需要强调所有参与者的责任。基于对网络空间安全的新认识,立法重点和高度发生了从对信息基础设施保护到国家关键基础设施保护的转移,强调物理空间安全与网络空间安全之间的关系,要求建立应急响应、检测预警机制,重视监控和信息共享,强调推动民营资本安全技术研究的重要性。

应当看到,网络空间安全的本质在于促进、维持经济繁荣。在这一点上美国与欧盟的安全理念也是一致的。因此,以发展、生存为核心的网络空间权理论随之产生。但人类社会对信息系统的依赖程度决定着网络空间权的内在结构。在高度信息化的国家,网络空间权强调人的生存权,而在发展中国家则强调的是人的发展权。在我国,信息化发展虽然不很平衡,但却发展很快。从目前我国发生的网络安全、网络犯罪案件来看,发达国家在不同阶段出现的网络信息安全问题在我国都有不同程度的反映。

“发展才是硬道理”。我们应当强调在信息系统和网络建设中同时解决安全问题,确立积极的风险预防和风险控制的法制原则,关注信息内容安全监控,树立安全使用信息系统和互联网络的新型法律文化理念。

从立法成本考虑,《网络与信息安全条例》的调整范围应当

包括以下主要内容 :(员) 网络信息安全应急保障关系 ;(圆) 信息共享分析、预警关系 ;(猿) 政府机构信息安全管理 ;(源) 通信运营机构的安全监管 ;(缘) 隐[illegible]的安全监管 ;(远) 隐[illegible](含大型商业机构) 的安全监管 ;(苑) 家庭用户及商业企业用户的安全责任 ;(愿) 网络与信息安全技术进出口监管 ;(怨) 网络与信息安全标准、指南、评估监管 ;(员园) 网络与信息安全研究规划 ;(员员) 网络与信息安全培训管理 ;(员圆) 网络与信息安全监控。

第二章从“公害”角度探究了计算机病毒防治的法律对策。

计算机病毒是现代人类社会的新型“公害”。蠕虫病毒具有堵塞网络的强复制能力,并可发动拒绝服务攻击,造成主干网络和服务缓慢、中断,直接威胁着信息基础设施的正常运行 ;“木马”病毒入侵系统,肆意破坏、窃取信息,严重危害了网络信息安全的“机密性”“完整性”“可用性”;邮件病毒附随的垃圾邮件等有害信息威胁着国家安全、社会稳定,进而导致了信息文化信仰危机。因此,计算机病毒已经成为我国网络信息安全的主要威胁,加强计算机病毒防治管理是维护网络信息安全的核心内容。

网络用户数和网络的应用程度与计算机病毒感染存在相应的递增关系。可以肯定,随着国家和社会对网络依赖程度的增强,计算机病毒对网络信息安全的威胁程度也必然会加大。

当前计算机病毒发展趋势具有易发性、攻击性和不可预见性的明显特征。

我国现行计算机病毒防治法中主要存在的问题有 :员)被动防治的理念导致错误的立法定位。立法只强调报告和减少损失,但缺乏评估、预测和分析病毒趋势的法律规定。圆)缺协调反病毒厂商服务的法律缺位, 市场良性竞争法律监管失控,导致

反病毒厂商之间、反病毒厂商和执法机关之间缺乏技术层面的信息共享,反病毒厂商产品彼此不兼容的恶性竞争时有发生,反病毒产业无法健康发展,用户安全利益无法保障。猿援网络服务提供者防范病毒的责任不明确。由于法律没有明确规定网络服务提供者的义务和责任,使网络信息安全风险最终由用户承担,在一定程度上也助长了病毒的泛滥。源援重视实体法中违法行为和危害后果的规定,轻视实施操作的程序法规定,导致了罪过处于无人受罚的尴尬境地,客观上助长了病毒制作与传播行为人的恶意心理。缘援对反病毒厂商,国外厂商的控制缺乏法律规制,国内反病毒产品及厂商服务市场未形成良性竞争,国外反病毒产品、厂商服务活动失控,使国家的网络信息安全面临严重威胁。

运用“黑洞”效应、协同理论和风险控制理论,有助于建立有效的计算机病毒防治法律体系。“黑洞”效应理论承认,病毒“公害”是信息化的伴随产物,要摒弃掠夺式的单一发展理念,注重可持续的多样化发展观,主导发展多模式的网络应用。否则,信息化发展的结果,不是推动国民经济的发展,而是有可能葬送人类社会的现代文明。

协同理论认为,系统要素在各自发挥作用时,必须借助于其他系统条件。假若能得到其他系统条件的配合,则可以发挥其应有的作用,反之则可能削弱其效能。协同理论的精髓在于坚持“积极防御”的战略思想,主张法律义务与技术规范之间的协同性,重视管理职责与法律责任的一致性,倡导网络用户之间的关联性。

风险控制理论是侵权行为法中的重要学说。按照风险控制理论,法律义务的分配及其责任配置,以公平、能力和机会为原

则,即谁给社会带来了风险,谁就应当承担减小风险和救济风险的责任,谁有能力、机会控制风险,谁从中受益,谁就应当承担风险责任,化解风险。

我们认为,我国网络信息安全病毒防治法律制度首先应当注意病毒公害的‘ 黑洞 ”效应,摒弃掠夺式的应用网络技术,促进多模式的网络发展,建立网络信息安全评估法律机制和保持“ 技术中立 ”的法律精神。

其次,应当摒弃现在封闭式的监管机制,建立开放式监管体制。从政府强制力的贯彻向所有用户的普遍参与过渡,建立病毒预测、分级预警、报告、共享、应急、分析、再预测的风险防治体系,体现积极防御和风险控制思想。

再次,应当积极引导和发展关键基础设施的稳健、自生成系统及病毒防治的基本技术,建立国家级病毒源代码库,按照协同理论,注重政府机构、反病毒厂商、研究机构、应急响应组织和用户之间的信息共享与合作,促进市场良性竞争,保证强有力的中央决策机构能够协调各方利益。

最后,开展病毒防治的国际合作。各国共同利益大于分歧,应当加强合作,通过采用相应的国际措施,基于统一或互惠的立法原则,最大程度地调查或起诉与计算机系统或数据相关的犯罪。

第三章从美国法令探究网络安全监控的正当性与必要性。

网络空间现已成为间谍、黑客攻击、诈骗等违法犯罪活动的场所。为了打击网上犯罪,必须对网络进行实时监控。

监控必然会引发与隐私权的冲突。然而二者孰轻孰重?自然应当以国家安全和社会公共安全优先于个人权益为原则。但这并不意味着对于隐私权的否定,而是主张在其与公权益发生

冲突时对隐私权进行适当的限制。同时,法律应当对监控的程序和手段作出严格的规定,以防范非法监控,侵犯公民私权益的情况发生。

美国两部主要的网络信息安全监控法令是 [illegible] (另一部是1986年的防治公共交通犯罪及道路安全法)和 [illegible] (另一部是[illegible])。[illegible] 允许政府获得传输中的有线或电子通讯的内容。[illegible] 关注实时寻址收集及其他与这些通讯相关的信息。法令对授权批准监控的主体、进行监控的合法期限、监控获得信息保存的期限、国家监控应通知被监控人、非法监控的民事责任、刑事责任、行政责任等都有明确具体的规定。这些规定有利于澄清 [illegible] 使用‘食肉者’软件所引发的有关监控程序等法律争议。

目前我国对于网络监控还没有专门的立法,其法律规范散见于《国家安全法》《刑法》及《人民警察法》《关于维护互联网安全的决定》等法律,其规定显得非常原则,过于简单,可操作性差。

我们认为,网络监控可以分为国家监控和企业监控。两者监控的法律依据不同。企业监控分为以下三个层次,一是国家授权,二是企业义务,三是自身利益保护;国家监控是人民法院、人民检察院、公安、国家安全等机关依据国家法律的授权实施的监控。两者监控的对象不同,法律依据不同,监控程序也不相同。企业监控仅仅是一般性的监控,履行法定的义务,及维护自身的财产利益。国家监控不仅包括一般性的监控,也包含特定的监控。最后两者损害赔偿责任不同。对于企业监控,滥用权利,必须承担责任。对于国家监控,依据国家赔偿法进行赔偿;被授权监控机关侵犯被监控人权益的由授权机关承担责任;在

监控手段别无选择、又必须监控的情况下，导致侵犯私权益的，可以适用除外责任。

第四章以“职能扩展”观，探索网络空间监管的法律体系。

市场失灵和网络这一公共财产本身的缺陷决定了对网络信息必须实行安全监管。网络作为人类所创造之物，国家法律完全可以利用网络技术性规则对其实行直接或间接管理。

监管即监察督促、管束，指依一定规则、方法或确立的模式，通过主管、检查，达到决定、确定或控制的目的。网络信息安全监管是国家机关运用行政手段或准立法、准司法手段对网络信息安全客体的控制。其有以下几个特点：法定性、系统性、技术性。网络安全监管应该首先保障网络安全，维护社会公共利益，进而实现信息社会的安全，在此大前提下再维护与协调主体之间的利益。

网络信息安全的监管对象主要有：国防、科研和经济等主要领域，通信运营机构、[illegible]（含大型商业机构）、家庭用户及商业企业用户、安全服务提供者（方案设计、施工、检测、认证、咨询、培训等）等。监管内容主要包括：网络信息安全应急保障关系、信息共享分析与预警关系、政府机构信息安全管理、通信运营机构安全监管、[illegible]的安全监管、[illegible]（含大型商业机构）的安全监管、家庭用户及商业企业用户的安全责任、网络与信息安全技术进出口监管、网络与信息安全标准、指南、评估监管、网络与信息安全研究规划、网络与信息安全培训管理、网络与信息安全监控。

从世界各国有关网络信息安全法律、法规以及相关政策可以看出，国际上对于网络信息安全进行监管已经成为普遍现象。国际网络信息安全监管制度有以下特点：[illegible]明确监管部门的职

责,重视部门间协调。国际设置的监管机构层次高。政策先行,基本上均由国家元首或总理直接领导,成立有关机构主管网络信息化建设。普遍重视信息安全政策、程序与业务的评估。如美国政府在制定安全政策、业务和程序时,都要进行评估。普遍重视技术培训。这是由网络信息安全监控的高技术性这一特点决定的。

我国网络信息安全立法在取得了巨大的进步同时,也存在很多缺陷。就监管制度而言,存在监管部门责任没有明确界定,缺乏有效的评估机制,监管方式单一,监管人员素质有待提高等问题。

采取何种监管模式,能够产生更有效、和谐的社会效果?一般而言,政府对监管模式的选择是在一个相对有限的范围内作出的,针对具体问题,所使用的方法会有所不同。我们认为经济领域,适用"产业监管"模式。在建立适度监管模式的同时,应该加强监管部门之间的协调,依据"谁运营、谁监管、谁负责"的原则,建立健全网络信息安全监管部门的责任体系,建立有效评估机制,实行有效成本监管,对监管政策、程序、业务与措施的适当性、成本与效益进行综合评价 建立有效的监管人员的技术培训,这一点上,普遍建议的四级安全知识培训计划值得我国借鉴。

第五章探索打击网络空间恐怖活动的网络信息安全共享法律制度。

网络信息安全共享是为了保障网络安全,以维护国家主权、社会公共利益以及社会成员的个体利益对信息资源的合法利用,或者说是对信息所有者在特定环境下的权利限制。本章首先提出了网络信息安全共享的概念及界定,信息安全共享即基

于信息资源的利用效率,在信息所有者与占有者及利用者之间形成的法律关系。

网络信息安全共享对于网络的健康发展至关重要。本章首先从心理学的安全需求理论、能力缺陷理论、成本—效率理论,产权理论入手,探讨了信息为网络安全共享的基础理论。

进而,通过分析美国信息立法共享的三个阶段,总结出美国立法中值得我国借鉴的地方。

我国的立法现状,问题比较突出。①对政府有关部门、在什么时间,什么特定情况下,什么方式,可发布什么样的信息,法律规定不明确。②信息网络测试评估信息的共享缺乏明确的法律规定。③政府监督管理部门、机构之间,由于制定信息安全标准的差异,难以进行信息共享。④企业之间的安全信息共享由于没有法律保障,共享难以实现。⑤共享与隐私存在着矛盾和冲突。⑥信息共享可能出现垄断法律问题。⑦安全信息的对外发布有缺陷,有些安全服务公司各自发布各自的安全信息,消费者无可适从。⑧信息共享与国家安全之间的冲突缺乏法律的协调。⑨知情不报的刑事责任,收集、使用的强制性特征,通报或者分析缺陷的责任无法落实。⑩政府机构之间在维护网络安全方面的信息共享同样也存有法律障碍。从政府机构的职能考虑,维护网络安全涉及政府多部门的利益。为了确保网络安全,综合分析相关安全事件信息,对危害网络安全作出快速反应,仅仅依靠国家安全和公安部门的力量已经不能适应当前网络活动恐怖国际化的客观形势要求。

最后提出相应的对策建议。

第六章针对网络信息安全技术,认为政府采购法的价值目标需要有新的定位。

加强对国产网络信息安全技术的政府采购是促进国产网络信息安全技术发展的一个有效途径，也是政府信息化过程中维护政府网络信息安全乃至国家安全的必然要求。我国《政府采购法》关于采购国货的规定是符合 宰栽的规定和国际惯例的。

安全价值目标、经济价值目标和发展价值目标是政府采购网络信息安全技术的三重价值目标，三价值之间层次分明，但又互相联系，呈互动态势。安全价值是三价值目标的核心，是第一目标，经济价值是第二目标，发展价值是第三目标。经济价值和发展价值服从于安全价值的要求，只能在保障安全的基础上考虑采购的经济性和民族产业的发展，没有安全保障的政府采购是谈不上经济与效率的，更无法促进民族产业的发展。反之，发展民族信息产业，提高国产网络信息安全技术水平，更能进一步维护信息安全，进而实现政府采购网络信息安全技术的经济价值目标。

国外关于政府采购网络信息安全技术的政策法律较多，如：世界贸易组织 员怨怨远年《政府采购协议》（[illegible]）、[illegible]年《美国产品购买法》、[illegible]年《武装服务采购法案》、[illegible]年《合同竞争法案》以及 [illegible]年《联邦采购合理化法案》、[illegible]年《联邦政府信息资源管理政策》（[illegible]号通告）及其附录 [illegible]《联邦自动化信息系统安全》（[illegible]）、[illegible]年《计算机安全法案》（[illegible]）、[illegible]年《政府信息安全改革法》（[illegible]）、[illegible]年《联邦信息安全管理法》（[illegible]）、俄罗斯《联邦信息、信息化和信息保护法》和

员怨怨缘年第 猿缘源号总统令。总结起来这些法律政策有以下特点：

第一，以法律的形式规定了对本国产品的采购，在这一基础上，强调对本国网络信息安全技术的采购，以维护网络信息安全和促进本国信息产业的发展；同时对国外产品的进口实施禁止或严格的资格审查。

第二，强调所采购的网络信息安全技术必须有安全质量证明。采取颁布标准、实行测评和认证制度等方式，对网络信息安全技术进行严格有效的管理。

第三，强调各个机构在采购网络信息安全技术之前应制定安全计划，对网络信息技术装置进行风险分析；安全装置投入运行前，进行设计审查和系统测试；对敏感应用系统进行定期审计或审查，以确保安全保护措施的适用性。

第四，明确了网络信息技术采购中，政府机构负责人的权限与责任：制定各机构采购需要的网络信息技术的政策和程序；授予各下属机构采购权；为机构采购网络信息技术提供指导；与联邦采购办公室进行采购政策方面的协调。即以行政管理的形式加强对网络信息技术采购与安全控制。

第五，规定对操作有敏感信息的政府计算机系统的人员进行安全意识的强制性定期培训，使其意识到安全的责任和实现的方式。

第六，严格按照政府采购的流程进行网络信息技术的政府采购，认为密封投标和竞争性谈判都是“完全和公开竞争”的方法，法律只是指出何时采用哪种采购方法。

第七，鼓励对商业化的网络信息安全技术进行政府采购。“承认商业化的信息安全产品提供了先进、有力和有效的信息安全策略，认识到私人设计建造并运营的市场方法可以保护重

要的信息基础设施,这些设施对于国防和国家经济安全是重要的。承认应当将选择特定的技术硬件和软件信息安全策略,留给商业化运营的私人机构。”

第八,为安全制定严格的标准和规则,强调在保证网络信息安全的前提下,避免不必要的网络信息安全技术的政府采购和重复建设,鼓励机构之间资源共享。

我国现行法中关于政府采购网络信息安全技术的法规政策有[1]《产品质量法》、[2]《招标投标法》、[3]《合同法》、[4]《国务院关于印发鼓励软件产业和集成电路产业发展若干政策的通知》、[5]《政府采购法》、[6]“中共中央办公厅、国务院办公厅转发《国家信息化领导小组关于加强信息安全保障工作的意见》的通知”(中办发[2003]27号)、[7]《政府采购评审专家管理办法》、[8]《集中采购机构监督考核管理办法》。

从总体上说,目前我国关于网络信息技术采购的法律政策不少,但对网络信息安全技术政府采购的规定较少,只是对网络信息安全技术的政府采购进行了原则性规定,缺乏操作性较强的网络信息安全技术采购实施管理办法。具体说来主要存在以下缺陷:

第一,政府采购网络信息安全技术的主体不够明确;

第二,政府采购网络信息安全技术的方式不够明确;

第三,政府采购网络信息安全技术的对象不够明确。

网络信息安全技术应纳入集中采购目录,由集中采购机构统一进行采购。集中采购机构应该加强对其工作人员网络信息安全技术的教育和培训,要求其具备专业资格。

出于对政府敏感信息安全的考虑,政府采购一方不能以招