网络安全法及其与相关立法的衔接
——我国《网络安全法（草案）》介评

Harmonization of Relationship between Cyberspace Security Law and the Related Legislation

张素伦
ZHANG Su-lun

【摘　要】　随着网络安全形势日益严峻，制定网络安全法已成为一种趋势。我国《网络安全法（草案）》的发布，为我国网络安全立法带来了契机。《网络安全法（草案）》的主要内容包括网络空间主权、网络安全战略、网络运行安全制度、网络信息安全制度、网络安全监测预警与应急处置制度等。为了实现未来《网络安全法》主要制度与相关立法文件的衔接，需要权衡以下几种关系：网络空间主权与网络安全国际合作，网络安全战略与网络安全立法，网络安全保障法与网络安全管理法，网络安全法与个人信息保护法，网络安全与信息化发展。

【关键词】　网络安全法　网络安全主权　网络信息安全
【中图分类号】DF49　【文献标识码】A　【文章编号】2095－9206（2016）03－0026－08

Abstract: As the situation of cyberspace security is becoming increasingly rigorous, making the cyberspace security law has become a trend. Laying down the draft Cyberspace Security Law brings the opportunity for Chinese cyberspace security law. Key elements of the draft Cyberspace Security Law include cyberspace sovereignty, cyberspace security strategy, system of safe operation of network, system of network information security and system of early warning and emergency disposal, etc. In order to achieve the connection between cyberspace security law and the related legislation, we need to balance the following relationships between cyberspace sovereignty and international cooperation in network security, cyberspace security strategy and cyberspace security law, cyberspace security protection and cyberspace security management, cyberspace security law and personal information protection law and cyberspace security and information technology development.

Key words: Cyberspace security law　Cyberspace security sovereignty　Network information security

［收稿日期］　2016－01－22
［作者简介］　张素伦，男，1975 年 3 月生，郑州大学法学院副教授，中国政法大学博士后，研究方向为网络安全法、竞争法。
［作者简介］　国家社科基金重大项目“互联网安全主要问题立法研究”（项目编号：14ZDC021）。

关于网络安全法，网络安全法制比较完善的西方发达国家，如美国制定了《国家网络安全保护法》，俄罗斯制定了《联邦信息、信息化和信息保护法》，欧洲议会和欧盟理事会则通过了《关于建立欧洲网络与信息安全局的第 460/2004 号条例》。而我国，尚未制定统一的网络安全法，这不利于应对日益严峻的网络信息安全威胁。2015 年 6 月，第十二届全国人大常委会第十五次会议初次审议了《网络安全法（草案）》，从而为我国网络安全立法带来了契机。

框架性的《网络安全法（草案）》在为未来立法预留空间的同时，也提出网络安全法与相关立法衔接中的一些问题，在对待这些问题时应把握“网络空间主权与网络安全国际合作”、“网络安全战略与网络安全立法”、“网络安全保障法与网络安全管理法”、“网络安全法与个人信息保护法”、“网络安全与信息化发展”的关系。

一、《网络安全法（草案）》的立法背景

（一）我国面临的网络安全形势日益严峻

当今世界，信息技术革命日新月异，互联网和信息化工作取得了显著发展成就，但在享受信息化建设带来的诸多便利时，网络的安全问题也日益引人关注。特别是“棱镜门”事件的曝光，让更多国家开始重视网络安全问题。从国内看，网络攻击、病毒传播、信息窃取等网络违法犯罪行为日益猖獗，维护网络安全、净化网络环境、保护用户利益的任务日益繁重。面对网络安全事件数量激增、网络安全威胁类型快速变化、网络安全威胁范围不断扩大的情势，我国不断加强网络安全保障，习近平总书记也做出“没有网络安全就没有国家安全，没有信息化就没有现代化”的重要指示。进行网络安全立法、构建网络安全保障制度的工作开始提上议事日程。

（二）国家筹划制定国家安全系列立法

2014 年初我国开始筹划制定一系列的涉及国家安全的法律，主要包括“国家安全法”、“网络安全法”、“反恐怖主义法”等。其中，（1）《国家安全法》已于 2015 年 7 月 1 日公布并实施。《国家安全法》第 25 条对网络安全保障做出了原则性规定；第 59 条则引入了国家安全审查和监管的制度、机制。（2）《反恐怖主义法》已于 2015 年 12 月 27 日公布并于 2016 年 1 月 1 日起实施。《反恐怖主义法》第 18 条明确了电信业务经营者、互联网服务提供者应当为依法进行防范、调查恐怖活动提供技术支持并予以协助；第 19 条规定了电信业务经营者、互联网服务提供者应当防止含有恐怖主义、极端主义内容的信息传播，一旦发现上述信息应当立即停止传输并予以删除；第 21 条也涉及电信、互联网等业务经营者、服务提供者对客户身份进行查验的义务。（3）《网络安全法（草案）》于 2015 年 7 月 6 日在中国人大网公布，向社会公开征求意见。在我国，网络空间安全秩序的构建需要《国家安全法》、《反恐怖主义法》以及未来《网络安全法》的协同作用，因此应及时完善该法律草案并出台《网络安全法》。

（三）各国和地区纷纷加强网络安全立法

为了应对日益严峻的网络安全形势，美国于 2014 年通过了《国家网络安全保护法》，强化了国土安全部的国家网络安全和通信集成中心在联邦部门和私营部门共享网络安全信息方面的重要作用，为立足国家层面部署和加强公共和私营部门网络安全信息共享提供了法律依据。日本于 2014 年颁布《网络安全基本法》，明确设立“网络安全战略本部”以统一协调各部门的网络安全政策，并对电力、金融等基础设施运营方落实网络安全的相关措施提出了要求。此外，俄罗斯于 2006 年制定《联邦信息、信息化和数据保护法》，加拿大于 2001 年出台《信息安全法》，作为保护本国网络安全的基本法律。欧盟也于 2013 年启动了《网络信息安全指令》立法，目前已进入最后的审议阶段。在世界各国和地区纷纷制定网络安全法的背景下，我国应加快网络安全立法的步伐。

二、《网络安全法（草案）》的框架结构和主要制度

（一）《网络安全法（草案）》的框架结构

《网络安全法（草案）》共七章内容，包含六十八个条文。其中，第一章为“总则”，包括

《网络安全法》的立法宗旨、适用范围、网络安全保护和监督管理机构、网络相关行业的自律等等。第二章为“网络安全战略、规划与促进”，包括网络安全战略、网络安全规划、网络安全标准体系、扶持重点网络安全技术产业和项目、网络安全宣传教育、网络安全技术人才的培养和交流等等。第三章为“网络运行安全”，包括网络运行安全的“一般规定”和“关键信息基础设施的运行安全”。主要涉及关键信息基础设施的界定、保护、“三同步”制度、运营者的安全保护义务、运营者采购网络产品或者服务等等。第四章为“网络信息安全”，这一部分明确了网络运营者收集、使用公民个人信息时应遵循的义务，依法负有网络安全监督管理职责的部门保护信息安全的职责，电子信息发送者发送电子信息时应当履行的安全管理义务。第五章为“监测预警与应急处置”，包括网络安全监测预警和信息通报制度，网络安全应急工作机制和应急预案，处置重大突发社会安全事件时可以在部分地区对网络通信采取限制等临时措施等等。第六章为“法律责任”，具体包括民事责任、行政责任和刑事责任。第七章为“附则”，主要涉及各种术语的界定、法律实施时间等内容。

（二）《网络安全法（草案）》的主要制度

1. 网络空间主权

《网络安全法（草案）》第 1 条开宗明义提出了“保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展”的立法宗旨，继《国家安全法》之后再次明确“网络空间主权”的概念，被誉为我国立法的一大创新。

2. 网络安全战略

在美国、日本、俄罗斯、韩国等纷纷将网络安全上升到国家层面，进而制定国家网络安全战略的背景下，我国《网络安全法（草案）》也设专章规定了“网络安全战略、规划与促进”，其中，第 11 条明确宣示“国家制定网络安全战略”。

3. 网络运行安全制度

这一制度包括网络运行安全的“一般规定”和“关键信息基础设施的运行安全”，涉及的内容主要为：（1）《网络安全法（草案）》第 17 条规定了“网络安全等级保护制度”；（2）《网络安全法（草案）》第 19 条规定了“网络关键设备和网络安全专用产品的认证和检测制度”；（3）《网络安全法（草案）》第 25 条规定了“关键信息基础设施安全保护制度”；（4）《网络安全法（草案）》第 30 条规定了“采购网络产品或者服务的安全审查制度”；（5）《网络安全法（草案）》第 32 条规定了“网络安全和风险的检测评估制度”。

4. 网络信息安全制度

《网络安全法（草案）》第 34 条至第 43 条要求建立健全用户信息保护制度、实现网络信息安全。这一部分明确了网络运营者收集、使用公民个人信息时应遵循的义务，依法负有网络安全监督管理职责的部门保护信息安全的职责，电子信息发送者发送电子信息时应当履行的安全管理义务。

5. 网络安全监测预警与应急处置制度

《网络安全法（草案）》第 44 条至第 50 条拟确立“网络安全监测预警与应急处置制度”，具体包括：网络安全监测预警和信息通报制度、网络安全应急工作机制和应急预案、处置重大突发社会安全事件时可以针对特定地区的网络通信实施临时限制措施等等。

三、《网络安全法（草案）》主要制度与相关立法的衔接

由于《网络安全法（草案）》属于框架性立法，该法律正式公布时，需要处理好与相关立法文件的衔接问题，具体表现为，其一，“网络安全法”的实施需要援引《国家安全法》、《突发事件应对法》等其他法律的相关条款，如《网络安全法（草案）》第 49 条规定：“因网络安全事件，发生突发事件或者安全生产事故的，应当依照《中华人民共和国突发事件应对法》、《中华人民共和国安全生产法》等有关法律的规定处置”。其二，《网络安全法（草案）》中的制度安排需要具体的立法规定进行细化，如《网络安全法（草案）》中的“网络安全等级保护制度”、“关键信息基础设施安全保护制度”、“采购网络产品

或者服务的安全审查制度”等都较为原则。三是《网络安全法（草案）》与非法律规范性文件之间的衔接，如“网络安全法”与“网络安全战略”的关系。尽管“网络安全战略”不属于法律范畴，但是由于两者之间关系的处理事关“网络安全法”实施的整体效果，在此一并略作分析。

通过对《网络安全法（草案）》框架结构和主要制度的梳理，可以从网络空间主权、网络安全战略、网络安全运行、网络信息安全、网络安全预警和应急等几个方面，来解读《网络安全法（草案）》与相关立法的衔接问题。

（一）在“网络空间主权”方面

当前，网络空间已经成为陆地、海洋、空间、太空之后的第五大主权领域，由于网络空间安全危险日趋显现，构建网络空间安全保障制度已经成为我国面临的迫切任务。而列明《网络安全法（草案）》立法宗旨的第 1 条便规定了“维护网络空间主权”。在现行立法中，我国 2015 年 7 月 1 日通过的《国家安全法》第 25 条首次提出了“维护国家网络空间主权、安全和发展利益”的措辞，而网络空间主权、安全和发展利益的实现，要取决于网络核心技术、关键基础设施、重点领域信息系统及数据是否安全可控，取决于网络攻击、网络入侵、网络窃密、散布违法有害信息等违法犯罪行为是否可防可治。其实，《网络安全法（草案）》第 1 条和《国家安全法》第 25 条都属于宣示性条款，宣示性条款虽被视为“软性”法律规定，但也有其必要性。这种条款宣示了国家网络安全立法的基本理念和基本原则，为我国网络安全保障制度的构建提供了法理依据。

由于两部法律都宣示了“网络空间主权”，有必要对《国家安全法》与未来颁布的《网络安全法》之关系进行说明：首先，两部法律都是由全国人大常委会制定，应属于同一位阶，不是上位法与下位法关系，也不是普通法与特别法的关系；其次，就立法宗旨而言，《国家安全法》保护的是国家安全利益，而《网络安全法》除了保护国家安全利益外，还保护社会公共利益、社会组织利益和个人利益，《网络安全法》调整对象的外延更宽；第三，《国家安全法》中有关国家安全利益的网络安全保障规定更为原则，往往需要《网络安全法》来付诸实施。两部法律还存在其他内容方面的交叉，同样参照上述思路进行处理。

（二）在“网络安全战略”方面

随着斯诺登“棱镜门”事件的曝光，我国不断加强网络安全保障，构建国家网络安全战略的重要性日益凸显。针对当前的网络安全情势，习近平总书记创造性地做出“没有网络安全就没有国家安全，没有信息化就没有现代化”的重要指示。有学者认为，中共中央成立网络安全和信息化领导小组，标志着中国已把网络安全提升到国家安全战略高度。[1]在此背景下，《网络安全法（草案）》第 11 条规定：“国家制定网络安全战略，明确保障网络安全的基本要求和主要目标，提出完善网络安全保障体系、提高网络安全保护能力、促进网络安全技术和产业发展、推进全社会共同参与维护网络安全的政策措施等。”

尽管《网络安全法（草案）》第 11 条积极倡导“国家制定网络安全战略”，但是现行立法中并找不到“网络安全战略”的规定，关于“网络安全战略”的原则性规定缺乏具体立法的衔接。与此同时，作为规范性文件的“网络安全战略”也没有制定出来，相关的文件如 2006 年中共中央办公厅、国务院办公厅印发的《2006—2020 年国家信息化发展战略》，该文件将“建设国家信息安全保障体系”作为我国信息化发展的战略重点之一，其具体目标包括：建立和完善信息安全等级保护制度、加强密码技术的开发利用、建设网络信任体系、加强信息安全风险评估、建设和完善信息安全监控体系、健全完善信息安全应急指挥和安全通报制度等。《2006—2020 年国家信息化发展战略》对我国未来制定“网络安全战略”具有一定指引作用。

（三）在“网络安全运行”方面

如前所述，通过对《网络安全法（草案）》的基本制度进行归纳，网络安全运行制度主要包括：网络安全等级保护制度、网络关键设备和网络安全专用产品的认证和检测制度、关键信息基础设施安全保护制度、采购网络产品或者服务的安全审查制度、网络安全和风险的检测评估制度等。就现行立法而言，仅有公安部等四部门制定的《信息安全等级保护管理办法》（公通字

[2007] 43 号），在一定程度上能够与“网络安全等级保护制度”进行衔接。《信息安全等级保护管理办法》第 2 条明确要求，国家制定并实施统一的信息安全等级保护管理规范和技术标准，并根据重要程度及遭受破坏后的损害程度，对信息系统的安全实行分等级保护。

需要注意的是，“网络安全等级保护”与“信息安全等级保护”的内涵不能等同，外延也有所区别。我国《网络安全法（草案）》将网络安全定义为“网络安全，是指通过采取必要措施，防范对网络的攻击、入侵、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络存储、传输、处理信息的完整性、保密性、可用性的能力”。显而易见，这种定义较为狭窄，没有包括信息安全。广义上的网络安全不仅涉及设备设施安全，也包括网络层安全和应用层安全（信息安全）。因此，无论从广义上，还是从狭义上来理解“网络安全”，其与“信息安全”的内涵和外延均有所不同。除此之外，《信息安全等级保护管理办法》发布于 2007 年，当时的网络安全形势、安全等级保护需求与当下存在较大差异，《信息安全等级保护管理办法》势必会滞后于网络安全的现实。

（四）在“网络信息安全”方面

在《网络安全法（草案）》第四章“网络信息安全”部分，第 34 条要求网络运营者建立健全用户信息保护制度，加强对用户个人信息、隐私和商业秘密的保护。第 35 条则明确了网络运营者收集、使用公民个人信息时应当遵循的原则和应当履行的义务。其他条款则规定了“个人信息处理规则、信息泄露通知”，“个人信息删除、更正权”，“个人信息不受窃取、非法获取、出售或非法提供权”。与《网络安全法（草案）》相衔接的为全国人大常委会《关于加强网络信息保护的决定》，如“二、网络服务提供者和其他企业事业单位在业务活动中收集、使用公民个人电子信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经被收集者同意，不得违反法律、法规的规定和双方的约定收集、使用信息。网络服务提供者和其他企业事业单位收集、使用公民个人电子信息，应当公开其收集、使用规则。”“三、网络服务提供者和其他企业事业单位及其工作人员对在业务活动中收集的公民个人电子信息必须严格保密，不得泄露、篡改、毁损，不得出售或者非法向他人提供。”

在网络信息安全规则方面，相比较而言，《关于加强网络信息保护的决定》比《网络安全法（草案）》更为周延。首先需要注意的是，《关于加强网络信息保护的决定》设定了“网络服务提供者和其他企业事业单位”的网络信息安全义务，而《网络安全法（草案）》主要关注“网络运营者”的网络安全义务，对网络安全监管部门的职责更是一笔带过，仅第 39 条中有所提及，即“依法负有网络安全监督管理职责的部门，必须对在履行职责中知悉的公民个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。”与此同时，《网络安全法（草案）》第 39 条中的责任主体应修改为“依法负有网络安全监督管理职责的部门及其工作人员”，因为监管部门的保密职责主要由其工作人员承担，且工作人员的行为并不全是职务行为，有些则是个人行为。

（五）在“网络安全预警与应急”方面

关于网络安全预警，《网络安全法（草案）》引入了网络安全监测预警和信息通报制度、网络安全应急制度。《网络安全法（草案）》要求发生网络安全事件时，县级以上网络安全保护部门应当及时启动应对网络安全事件之预案，及时向社会发布与公众有关的警示信息。同时规定，为了维护国家安全和社会公共秩序，在处置突发性重大社会安全事件时，国务院或经国务院批准的省级人民政府，可以针对特定地区的网络通信实施临时限制措施。

从现有的立法文件来看，尚欠缺对网络安全预警制度和应急制度的规定。但在《2006—2020 年国家信息化发展战略》中，对网络安全预警制度和应急制度进行了初步设计。如在“四、我国信息化发展的战略重点”下的“建设国家信息安全保障体系”部分，提出如下规划：“建设和完善信息安全监控体系，提高对网络安全事件应对和防范能力，防止有害信息传播。高度重视信息安全应急处置工作，健全完善信息安全应急指挥和安全通报制度，不断完善信息安全

应急处置预案。从实际出发，促进资源共享，重视灾难备份建设，增强信息基础设施和重要信息系统的抗毁能力和灾难恢复能力。”上述规划为我国未来的网络安全预警和应急立法留下一定空间，并初步厘定了网络安全预警和应急立法的基本体系。

四、《网络安全法（草案）》与相关立法衔接时应权衡几种关系

前文表明，就《网络安全法（草案）》主要制度与相关立法衔接的实际效果而言，主要表现为三种情形，第一，《网络安全法（草案）》基本制度能够与现行立法的衔接。这种情形是指现行立法能够与《网络安全法（草案）》的规定相衔接，或者能够细化有关立法中的框架性规定。如前所述，现有的立法格局尚无法实现法律衔接的应然效果。第二，《网络安全法》基本制度难以与现行立法衔接。这种情形是指现行立法中虽然有相关规定与《网络安全法（草案）》基本制度相对接，但是由于现行立法的滞后性，相关的规定也表现得不合时宜，需要进一步完善。第三，《网络安全法》基本制度缺乏与相关立法的衔接。这种情形是指现行立法存在相关规定，但是《网络安全法（草案）》中缺少相关制度，或者指《网络安全法（草案）》的抽象条款缺乏可操作性，亟待具体规则的指引。如国务院发布了《商用密码管理条例》，“密码应用管理制度”对于加强商用密码管理、保护信息安全、保护公民和组织的合法权益、维护国家的安全和利益，具有重要意义。“密码应用管理制度”是各国网络安全法的必要组成部分，而我国《网络安全法（草案）》中缺少“密码应用管理制度”，显得不够完整。

因此，为了提高“网络安全法”的立法质量、增强“网络安全法”的实施效果，应在《网络安全法（草案）》中对网络安全主要制度与相关立法的衔接做出前瞻性安排。在进行这种预见性制度设计时，有必要对以下几种关系进行权衡。

（一）网络空间主权与网络安全国际合作

在《国家安全法》之后，我国《网络安全法（草案）》第 1 条再次明确宣示了“网络空间主权”。可见，关于网络安全保障，不能仅仅关注国内的网络安全。实际上，从境外发起的针对我国的网络入侵，其危险性、危害性更大，甚至要比国内的网络安全管理问题更重要。如有的学者认为，为了维护网络空间主权，可将《网络安全法（草案）》第 2 条修改为：“在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。在中华人民共和国境外使用网络，侵犯中华人民共和国网络空间主权，侵犯中华人民共和国国家安全、社会公共利益及公民、法人和其他组织的合法权益的，可以适用本法。在中华人民共和国境外使用网络，即使行为地法律不认为是违法犯罪的，中华人民共和国有权在网络主权范围内采取相应的封锁、过滤等管制措施。”[2]同时，也要避免因管辖权的扩大而引起国际上的强烈反应，平衡国内安全与国外威胁的关系，实现网络空间安全。事实上，我国《网络安全法（草案）》也推崇网络安全国际合作，如第 5 条规定：“国家积极开展网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面的国际交流与合作，推动构建和平、安全、开放、合作的网络空间。”

众所周知，在网络时代，网络空间是国家经济社会运行的重要载体，“没有网络安全就没有国家安全”。联合国信息社会世界峰会通过的《日内瓦原则宣言》明确表示：“互联网公共政策的决策权是各国的主权”。但各国在网络空间主权问题上的立场并不完全一致，如中美之间的一大核心分歧在于网络空间管理政策上的“自由度”问题，美方指责中方妨害互联网自由，而中方坚持本国的正当网络主权行为不容他国置喙。[3]对待这一问题，既要坚持“网络空间主权”，也要提倡“网络安全国际合作”，如我国国家互联网信息办公室主任指出，“中美应互相尊重而不是对立指责。在网络空间，应当彼此尊重网络主权，尊重对互联网治理模式的选择，尊重在网络领域的重大关切，尊重在网络文化上的差异，深入沟通，增进理解，扩大共识”[4]。

（二）网络安全战略与网络安全立法

网络安全战略是对一个国家或地区网络安全战略目标、战略重点、行动计划的整体设计，美

国、欧盟、日本、俄罗斯、韩国等国家和地区都制定了国家层面的网络安全战略。而有的国家既制定了网络安全战略，又颁布了网络安全立法，如美国于 2011 年出台了《网络空间安全法案》、《网络空间行动战略》，2014 年又颁布《国家网络安全保护法》、《联邦信息安全管理法案》；日本制定了网络安全战略，即《保卫国民信息安全战略 2010—2013》，并于 2014 年发布了《网络安全基本法》。一般而言，网络安全战略是国家行为，而网络安全立法是调整人与人之间社会关系的行为规范。各个国家往往在网络安全法中对“网络安全战略”规定宣示性条款，而由官方制定网络安全战略规划来设计网络安全战略的目标、重点、实施等重要问题。

相比较而言，网络安全战略侧重于产业发展，网络安全立法侧重于规则设计，网络安全战略需要随着情势变化而适时进行调整，网络安全立法则要求尽量作出前瞻性安排以确保稳定性和可预见性。网络安全战略的基本范畴为：战略目标、战略重点、行动计划等；而网络安全立法的基本范畴为：主体、权利义务（职权职责）、法律责任等。网络安全战略的主要内容为：国内外网络安全的基本形势、网络安全战略的指导思想、网络安全战略目标、网络安全战略重点、网络安全战略行动、网络安全战略的保障措施等；而网络安全立法的主要内容为：网络运行安全、网络信息安全、监测预警与应急处置、法律责任等。因此，网络安全战略与网络安全立法不能等同，更无法彼此替代。我国网络安全法颁布后，不但不会停止制定国家层面网络安全战略的步伐，而且会倒逼网络安全战略尽快出台。

（三）网络安全保障法与网络安全管理法

我国未来的网络安全法应为“网络安全保障法”，而不应将其定位为“网络安全管理法”。但我国《网络安全法（草案）》整体上呈现出“重政府职权、职责而轻公民、法人和其他组织权利、义务”的色彩，草案欠缺网络安全保障方面的内容，实为网络安全管理法。正如有的学者所言，从《网络安全法（草案）》制度构架来看，几乎全部都是政府授权性条款和企业、公民的义务性条款。仅有第 9 条提到“国家保护公民、法人和其他组织依法使用网络的权利”，第 54 条与相关条款中提到“保护公民个人信息的权利”。草案重在描述政府如何管理，以及企业和个人如何配合政府管理。从本质上讲，这种立法体例和制度安排明显将“网络安全法”变成了“网络安全管理法”。[2]

《网络安全法（草案）》中的“网络安全运行”部分，更是体现出“重管理，轻保护”及“重实体，轻程序”的突出问题。如对于《网络安全法（草案）》中的“网络安全等级保护制度”，规定了“网络安全等级保护的具体办法由国务院规定”；对于“网络关键设备和网络安全专用产品的认证和检测制度”，规定了“国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录”；对于“关键信息基础设施安全保护制度”，规定了“关键信息基础设施安全保护办法由国务院制定”；对于“采购网络产品或者服务的安全审查制度”，也指出“具体办法由国务院规定”，等等。这种“重赋权赋能，轻保护程序”的立法理念，无疑会引起人们对公权侵犯私权的担忧及对《网络安全法（草案）》定位的质疑。在立法过程中，应改变上述“重管理，轻保护”的思路，使《网络安全法（草案）》的立法理念回归本位。

（四）网络安全法与个人信息保护法

广义上的网络安全可以划分为国家安全、公共安全和个人安全三个层面。网络安全，首先需要保障国家安全和公共安全，要将网络安全上升到战略高度，国家安全得不到保障，个人安全也无从谈起。因此，从立法模式来看，根据我国网络安全的实际情况，在进行网络安全立法时，可以借鉴西方国家的立法经验，采用分别制定“网络安全法”和“个人信息保护法”的立法模式。[5]两部法律的侧重点有所不同，“网络安全法”侧重于保护国家层面的网络安全，保护的对象不仅包括作为硬件设施的物理网络，而且包括作为内容的网络信息等；而“个人信息保护法”则重点保护公民个人的信息安全。

此外，“网络安全法”的立法宗旨与“个人信息保护法”也存在一定冲突，我国《网络安全法（草案）》与其糅合“网络安全法”和“个人信息保护法”，倒不如减少“个人信息保护法”方面的条款。这样《网络安全法（草案）》的立

法理念变得更为协调，也为今后制定单独的“个人信息保护法”预留立法空间。如有的学者认为，从价值取向方面，个人信息保护立法和网络安全立法存在明显区别。个人信息保护法的价值取向是维护公民的个人信息权等基本权利，规范个人信息的合理流动和秩序；网络安全法本质是为了维护国家安全、社会安定和不特定公民权益，而对包括个人信息权在内的公民私权予以必要限制，某种程度上这构成了对个人信息安全的威胁。由此导致在同一部法律的《草案》中，存在网络安全保护和个人信息保护的内在价值冲突，这样大篇幅规定个人信息保护的基本制度，一方面在一定程度上造成了立法资源的浪费，另一方面也挤压了未来专门出台《个人信息保护法》的立法空间。[6]

（五）网络安全与信息化发展

《网络安全法（草案）》引入了网络安全监测预警和信息通报制度、网络安全应急制度，尤其是第 50 条赋予相关主管部门处置违法信息、阻断违法信息传播的权力，即“因维护国家安全和社会公共秩序，处置重大突发社会安全事件的需要，国务院或者省、自治区、直辖市人民政府经国务院批准，可以在部分地区对网络通信采取限制等临时措施。”这一条款被学界解读为“重大突发事件，政府可限制网络”。对限制网络条款的适用，应结合网络安全与信息化发展的关系进行理解。从我国《网络安全法（草案）》的立法理念来看，应坚持“网络安全与信息化发展并重”的基本原则。

诚然，网络安全和信息化是“鸟之两翼、车之双轮”，安全是根本保障，发展始终是硬道理。《网络安全法》的出台，既要有利于网络安全，更要有利于网络行业发展。关于网络安全与信息化之间的关系，须坚持网络安全与信息自由并重，既要规范网络空间安全，又要保障网络信息依法有序自由流动。网络信息自由包含信息生产的自由、信息传播的自由和信息消费的自由，但网络信息自由是相对的，而不是绝对的，网络空间已经从自由走向控制，但是控制的同时又要保留部分自由。我国未来的《网络安全法》既要保障网络安全，也要为中国互联网企业的发展创造条件，进而促进网络技术创新和信息化持续健康发展。因此，《网络安全法（草案）》中限制网络条款应审慎适用。

综上，通过对《网络安全法（草案）》的框架结构和主要制度进行梳理，可以将其中的主要制度归纳为：网络空间主权、网络安全战略、网络运行安全制度、网络信息安全制度、网络安全预警与应急制度等。这些制度与现行立法衔接或者与未来立法对接时，应权衡“网络空间主权与网络安全国际合作”、“网络安全战略与网络安全立法”、“网络安全保障法与网络安全管理法”、“网络安全法与个人信息保护法”、“网络安全与信息化发展”的关系，从而最大程度发挥网络安全法的功能，有效应对我国日益严峻的网络安全威胁。

参考文献

[1] 邢若宸．专家：中国已把网络安全提升到国家安全战略高度［EB/OL］．［2014－02－27］．http：//china.haiwainet.cn/n/2014/0227/c345646-20340253.html.

[2] 谢君泽．关于《网络安全法（草案）》的几个重大问题［EB/OL］．［2015－07－19］．http：//www.aisixiang.com/data/90578.html.

[3] 檀有志．中国网络安全法草案的外扬与内抑［EB/OL］．［2015－08－04］．http：//www.ftchinese.com/story/001063323?page＝rest.

[4] 张蔚然．中国阐述中美互联网合作五大主张 吁尊重网络主权［EB/OL］．［2014－12－03］．http：//www.chinanews.com/gn/2014/12－03/6837827.shtml.

[5] 孙佑海．论我国网络安全面临的十大问题和立法对策［J］．中国信息安全，2014（10）：42.

[6] 丁道勤．“上天入地”，还是“度权量利”［EB/OL］．［2015－07－27］．http：//www.vchale.com/iPolicyLaw/209238633_1_b0a591c570b0ddca1856f86ebd871aef.html.

（责任编辑：于文豪　赵建蕊）