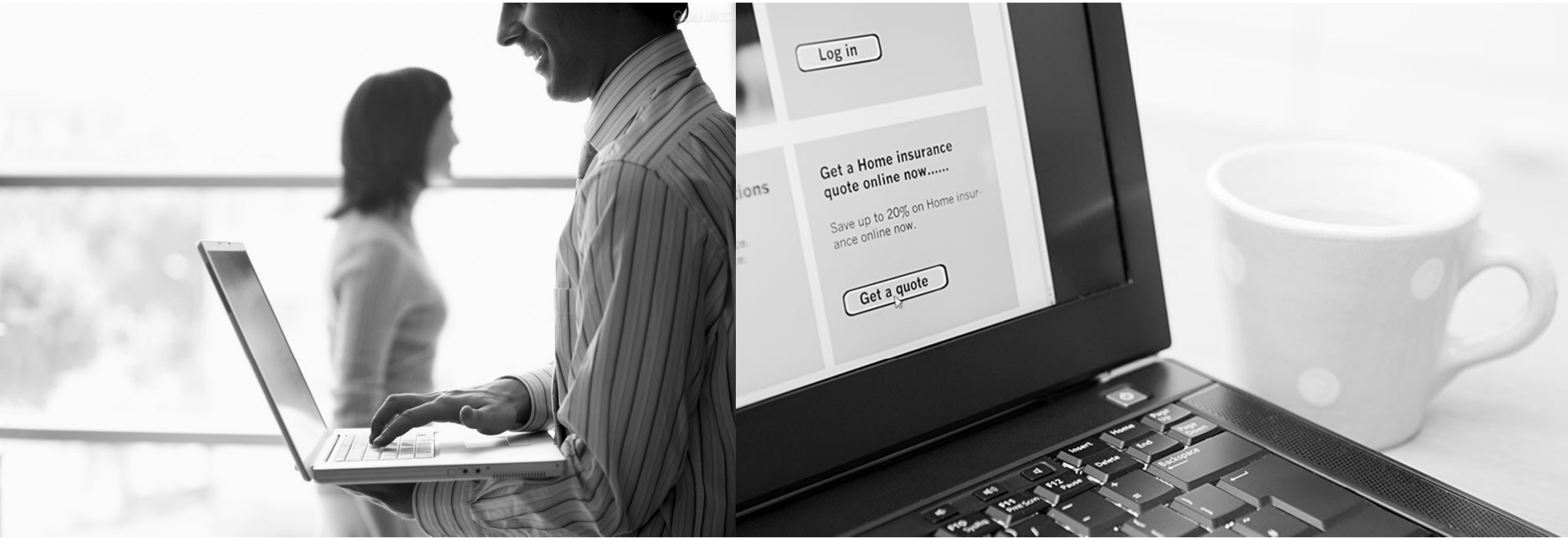
ANY. 安言咨询



新形势下企业的网络安全挑战和应对

-关于《中华人民共和国网络安全法》解读

目录

CONTENTS

[1] 立法背景

网络安全面临的威胁

➢ 网络安全已成为关系国家安全发展和人民群众切身利益的重大问题

当前，网络和信息技术迅猛发展，已经深度融入我国经济社会的各个方面，极大地改变和影响着人们的社会活动和生活方式，在促进技术创新、经济发展、文化繁荣、社会进步的同时，网络安全问题也日益凸显。

- 网络入侵、网络攻击等非法活动，严重威胁着电信、能源、交通、金融以及国防军事、行政管理等重要领域的信息基础设施的安全，云计算、大数据、物联网等新技术、新应用面临着更为复杂的网络安全环境。
- 非法获取、泄露甚至倒卖公民个人信息，侮辱诽谤他人、侵犯知识产权等违法活动在网络上时有发生，严重损害公民、法人和其他组织的合法权益。
- 宣扬恐怖主义、极端主义，煽动颠覆国家政权、推翻社会主义制度，以及淫秽色情等违法信息，借助网络传播、扩散，严重危害国家安全和社会公共利益。

典型网络犯罪案例

湖北十堰侦破刘某等人“伪基站”通讯网络诈骗案

2016年3月，湖北十堰市公安机关发现，有人利用“伪基站”发送诈骗短信实施诈骗。在公安部的统一指挥下，湖北、福建等地公安机关抽调30名精干警力，历经81天艰苦侦查，查清了以刘某、陈某、史某、黄某为首的犯罪团伙和活动轨迹制售窝点，一个专门面向全国及缅甸等国销售伪基站“核心配件”电脑主板的特大职业化犯罪团伙逐渐浮出水面。5月26日，多地同时收网，抓获刘某等15名犯罪嫌疑人，缴获“伪基站”设备成品和半成品共计300余套；生产“伪基站”设备核心主板窝点2个，扣押伪基站的“核心配件”电脑主板1100余套以及多条生产线，涉案资金达300余万元。经查，2015年8月以来，犯罪嫌疑人黄某、史某、刘某等人秘密开设地下“黑工厂”加工生产可以伪装安置在汽车音响中的新型伪基站“核心配件”电脑主板，然后通过网络联系买家，销往全国23个省市以及缅甸等国制售窝点，从中牟取暴利。

典型网络犯罪案例

黑龙江大庆侦破辛某等人破坏计算机信息系统案

2015年3月初，黑龙江大庆网安部门接到腾讯公司报案称，有人在大庆市利用计算机“外挂”从事某平台游戏“刷币”活动。经过一个多月的缜密侦查，大庆公安网安部门成功打掉了当地人员辛某经营的利用“外挂”程序游戏代练工作室4个，并在河南南阳成功抓获专门编写该游戏“外挂”程序的人员5名。经查，2014年10月份以来，辛某等人出资在网上联系河南郑州市“外挂”程序作者陈某等人，使用“外挂”程序刷取腾讯公司某平台游戏金币出售从而获利，累计涉案价值300余万元。目前，该案已刑事拘留犯罪嫌疑人16人，取保候审2人，相关涉案人员已经移送检察机关批准逮捕。

典型网络犯罪案例

辽宁沈阳侦破方某冒充信用卡卡主套现网络诈骗

2016年1月，辽宁沈阳公安机关接到银行报案，称“有多名储户补办信用卡套现，账面一直是处于欠款状态”，银行工作人员经过核实，这些储户都是被冒名补卡盗刷，并非本人套现。沈阳公安机关经过3个月的侦查，4月20日，在沈阳市和阜新市成功抓获方某等4名犯罪嫌疑人，缴获作案用电脑2台，手机16部，另抓获信用卡非法套现嫌疑人1名。经审讯，2015年7月以来，方某伙同杨某、刘某等5人在网上大量收购含有信用卡资料的公民个人信息，冒充卡主诈骗银行。据交代，该团伙先后补办了40余张信用卡在POS机上盗刷金额达150万元。

典型网络犯罪案例

安徽滁州侦破李某非法获取公民个人信息案

2015年12月，安徽滁州网安部门工作发现，支付一定费用后，可以通过“XX网”网站按照用户名查询各类网络服务的密码，该网站涉嫌侵犯公民个人信息犯罪。经滁州网安部门周密部署，抓获李某等犯罪嫌疑人2名，查明涉案金额6万余元、收缴非法获取的公民个人信息约30亿条。据李某交代，2014年以来，其在互联网上大量购买、搜集、汇总各类邮箱、论坛、网银等网络服务的账号密码，并搭建“XX网”网站，伙同施某公开出售数据查询服务，共计牟利6万余元。目前，该案抓获的2名犯罪嫌疑人均已移送起诉。

典型网络犯罪案例

贵州破获1.17亿假冒公安机关电信诈骗案

2015年12月，贵州黔南州都匀市经济开发区某财务主管杨某先后接到自称是银行和公安机关的电话，称杨某掌握的账号“涉嫌犯罪”，要求对其资金进行清查，在近一周的时间内，杨某单位两个对公账户上的总计1.17亿资金被转走。案件发生后，贵州公安机关立即调集500多名警力全力开展侦办，立即对上万个涉案账户实施紧急止付，挽回经济损失1亿多元。同时，确定该诈骗团伙话务窝点位于非洲乌干达境内，团伙主要头目均为台湾人。在进一步确定嫌疑人后，办案人员分赴北京、上海、广东等地，共抓获各类犯罪嫌疑人62名，其中包括台湾犯罪嫌疑人10名。此外，公安机关还通过该案串并、侦破涉及全国26个省市的180余起电信诈骗案。

信息安全相关法律法规

➢ 信息安全法律现状

我国信息网络安全立法体系框架分为个层面

- 法律
- 行政法规
- 地方性法规、规章
- 规范性文件

信息安全相关法律法规

- 国家法律
  - 《维护互联网安全的决定》【2009-8-27修正】
  - 《加强网络信息保护的决定》【2012-12-28】
  - 刑法【2015年8月29修正】
  - 治安管理处罚法【2005-8-28】
- 行政法规
  - 国务院令147号：《中华人民共和国计算机信息系统安全保护条例》
  - 国务院令195号：《中华人民共和国计算机信息网络国际联网管理暂行规定》
  - 国务院令291号：《中华人民共和国电信条例》
  - 国务院令292号：《互联网信息服务管理办法》
  - 国务院令339号：《计算机软件保护条例》
  - 国务院令363号：《互联网上网服务营业场所管理条例》等。

信息安全相关法律法规

信息安全相关部门规章

- 计算机信息系统安全专用产品检测和销售许可证管理办法【1997-12-12】 - 公安部
- 计算机信息网络国际联网安全保护管理办法【1997-12-30】-公安部
- 计算机信息系统保密管理暂行规定【1998-02-26】-国家保密局
- 计算机信息系统集成资质管理办法【1999-12-07】 - 信息产业部
- 计算机信息系统国际联网保密管理规定【2000-01-01】-国家保密局
- 计算机病毒防治管理办法【2000-04-26】 - 公安部
- 互联网电子公告服务管理规定【2000-11-07】 - 信息产业部
- …

信息安全相关地方法规

- 北京市党政机关计算机网络与信息安全管理办法【2001-11-15】
- 重庆市计算机信息系统安全保护条例【2001-12-07】
- 淮南市计算机信息系统安全管理办法【2001-12-25】
- 重庆市电信条例【2002-03-27】
- 江西省电信条例【2003-03-31】
- 广东省计算机信息系统安全保护管理规定【2003-04-08】
- …

信息安全相关法律法规

➢ 现有的互联网法律法规存在的主要问题

- ◆ **一是层级低。**缺乏上位法,现有关于互联网业务管理、网络与信息安全、用户个人权益保护方面的法律文件均为部门规章,对违法行为的处罚力度不够、执行力较弱、实施效果欠佳。
- ◆ **二是不健全。**如针对电子商务、信息资源开放利用、用户信息保护等领域仍未有明确的法律制度予以规范。
- ◆ **三是“碎片化”现象突出。**传统行业管理部门的法律法规缺乏对互联网的兼容性和包容性,导致“政出多门”,难以形成约束合力,在网络基础设施保护、互联网信息服务市场准入管理等领域,都不同程度上存在法律条块分割、部门多头管理等现象。
- ◆ **四是部分立法需要尽快修订完善或出台新的制度。**如《电信条例》中关于电信业务分类、互联网信息服务市场准入、无线电频率规划分配制度等,在不同程度上存在着与实践管理脱节的问题,亟需调整和完善。

网络安全法立法的必要性

- **制定网络安全法，是落实党中央决策部署的重要举措。**

  制定网络安全法，是落实总体国家安全观和党中央决策部署，适应并推动国家网络安全工作，维护国家网络空间主权、安全和发展利益的重要举措。

- **制定网络安全法，是维护网络安全的客观需要。**

  中国是一个网络大国，也是遭受网络安全威胁最严重的国家之一，迫切需要建立健全网络安全法律制度，提高全社会的网络安全保护意识和能力，应对各种网络安全风险和威胁，使我们的网络更加安全、开放、便利，更加充满活力。

- **制定网络安全法，是维护广大人民群众切身利益的必然要求。**

  制定网络安全法，是回应人民群众的呼声和期待，将最广大人民群众在网络空间的利益维护好、实现好、发展好。

- **制定网络安全法，是参与互联网国际竞争和国际治理的必然选择。**

  我国在互联网领域的竞争力和话语权逐渐增强，为了更好地参与互联网国际竞争和国际规则的定制，必须制定和完善国内制度规则，积累中国制度经验。

网络安全法立法过程

《网络安全法》是我国第一部全面规范网络空间安全管理方面问题的基础性法律，是我国网络空间法治建设的重要里程碑，是依法治网、化解网络风险的法律重器，是让互联网在法治轨道上健康运行的重要保障。《网络安全法》将近年来一些成熟的好做法制度化，并为将来可能的制度创新做了原则性规定，为网络安全工作提供切实法律保障。

1
- 2013年10月
- 立法规划

2
- 2014-2016
- 立法工作计划

1
- 2015年6月26日
- 一审

2
- 2016年6月28
- 二审

3
- 2016年10月31日
- 三审

4
- 2016年11月7日
- 发布

5
- 2017年6月1日
- 实施

[2] 网安法纵览

法律地位

➢ 法律体系

《网络安全法》构成我国网络空间安全管理的基本法律，与《国家安全法》、《反恐怖主义法》、《刑法》、《保密法》、《治安管理处罚法》、《关于加强网络信息保护的决定》、《关于维护互联网安全的决定》、《计算机信息系统安全保护条例》、《互联网信息服务管理办法》等现行法律法规共同构成中国关于网络安全管理的法律系统。

➢ 配套法规

《网络安全法》是基础性法律。国务院及相关的部门会制定和颁布一系列的配套法律法规，比如网络安全等级保护制度、关键信息基础设施的认定和保护办法、数据跨境传输的安全评估办法、网络产品和服务的国家安全审查制度等，数量上可能会达十余部。

适用范围

➢ 法律适用与管辖

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。

➢ 域外管辖

《网络安全法》采取了有限的域外管辖原则，依照法**七十五条**，境外的主体实施入侵或攻击境内关键信息基础设施的活动，造成严重后果的，依法追究法律责任，且中国执法机关可实施财产冻结等制裁措施，这是为应对日益严重的全球网络安全威胁的需要。

基本原则

第一，网络空间主权原则。《网络安全法》第1条“立法目的”开宗明义，明确规定要维护我国网络空间主权。网络空间主权是一国国家主权在网络空间中的自然延伸和表现。第2条明确规定《网络安全法》适用于我国境内网络以及网络安全的监督管理。这是我国网络空间主权对内最高管辖权的具体体现。

第二，网络安全与信息化发展并重原则。《网络安全法》第3条明确规定，国家坚持网络安全与信息化并重，遵循积极利用、科学发展、依法管理、确保安全的方针；既要推进网络基础设施建设，鼓励网络技术创新和应用，又要建立健全网络安全保障体系，提高网络安全保护能力，做到“双轮驱动、两翼齐飞”。

第三，共同治理原则。《网络安全法》坚持共同治理原则，要求采取措施鼓励全社会共同参与，政府部门、网络建设者、网络运营者、网络服务提供者、网络行业相关组织、高等院校、职业学校、社会公众等都应根据各自的角色参与网络安全治理工作。

立法定位

- 以发现、消除网络安全威胁和风险，提高恢复能力为轴心。

- **“发现”**包括网络安全漏洞的掌控、网络安全威胁和风险的实时全面共享、侦查、监测预警和供应链安全等；
- **“消除”**包括及时动态地研判处置网络攻击，实施精准打击的同时允许有条件的攻击反制；
- **“恢复”**侧重网络安全态势感知和网络攻击之后的应对恢复，保护有关各方的合法权益，提高各方对国家安全和社会稳定的信息。

立法要点

一、《网络安全法》提出制定网络安全战略，明确网络空间治理目标，提高了我国网络安全政策的透明度

《网络安全法》第4条明确提出了我国网络安全战略的主要内容，即：明确保障网络安全的基本要求和主要目标，提出重点领域的网络安全政策、工作任务和措施。第7条明确规定，我国致力于“推动构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的网络治理体系。”这是我国第一次通过国家法律的形式向世界宣示网络空间治理目标，明确表达了我国的网络空间治理诉求。上述规定提高了我国网络治理公共政策的透明度，与我国的网络大国地位相称，有利于提升我国对网络空间的国际话语权和规则制定权，促成网络空间国际规则的出台。

立法要点（续）

二、《网络安全法》进一步明确了政府各部门的职责权限，完善了网络安全监管体制

《网络安全法》将现行有效的网络安全监管体制法制化，明确了网信部门与其他相关网络监管部门的职责分工。第8条规定，国家网信部门负责统筹协调网络安全工作和相关监督管理工作，国务院电信主管部门、公安部门和其他有关机关依法在各自职责范围内负责网络安全保护和监督管理工作。这种“1+X”的监管体制，符合当前互联网与现实社会全面融合的特点和我国监管需要。

立法要点（续）

三、《网络安全法》强化了网络运行安全，重点保护关键信息基础设施

《网络安全法》第三章用了近三分之一的篇幅规范网络运行安全，特别强调要保障关键信息基础设施的运行安全。关键信息基础设施是指那些一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的系统和设施。网络运行安全是网络安全的重心，关键信息基础设施安全则是重中之重，与国家安全和社会公共利益息息相关。为此，《网络安全法》强调在网络安全等级保护制度的基础上，对关键信息基础设施实行重点保护，明确关键信息基础设施的运营者负有更多的安全保护义务，并配以国家安全审查、重要数据强制本地存储等法律措施，确保关键信息基础设施的运行安全。

立法要点（续）

四、《网络安全法》完善了网络安全义务和责任，加大了违法惩处力度

《网络安全法》将原来散见于各种法规、规章中的规定上升到人大法律层面，对网络运营者等主体的法律义务和责任做了全面规定，包括守法义务，遵守社会公德、商业道德义务，诚实信用义务，网络安全保护义务，接受监督义务，承担社会责任等，并在“网络运行安全”、“网络信息安全”、“监测预警与应急处置”等章节中进一步明确、细化。在“法律责任”中则提高了违法行为的处罚标准，加大了处罚力度，有利于保障《网络安全法》的实施。

立法要点（续）

五、《网络安全法》将监测预警与应急处置措施制度化、法制化

《网络安全法》第五章将监测预警与应急处置工作制度化、法制化，明确国家建立网络安全监测预警和信息通报制度，建立网络安全风险评估和应急工作机制，制定网络安全事件应急预案并定期演练。这为建立统一高效的网络安全风险报告机制、情报共享机制、研判处置机制提供了法律依据，为深化网络安全防护体系,实现全天候全方位感知网络安全态势提供了法律保障。

[3] 网安法解读

概述

目标

- 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、法人和其他组织合法权益，促进经济社会信息化健康发展

范围

- 在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全监督管理的活动，适用本法。

总览

- 法律条文：共7章，79条
- 2016年11月7日发布
- 2017年6月1日起施行

网络安全法大纲概要

第一章 总则	14条规定	简述法律目的，范围，总则， 部门职责，总体要求等
第二章 网络安全支持与促进	6条规定	定义国家直属部门、政府在推动网络安全工作上的职责
第三章 网络运行安全	19条规定	定义网络运营者与关键信息基础设施的运行安全规定
第一节 一般规定	10条规定	针对网络运营者的网络运行安全要求与职责规定
第二节 关键信息基础设施的运行安全	9条规定	针对关键信息基础设施的安全规定与保护措施要求
第四章 网络信息安全	11条规定	定义个人信息保护的保护规定
第五章 监测预警与应急处置	8条规定	定义国家网络安全监测预警与汇报机制
第六章 法律责任	17条规定	定义处罚规定
第七章 附则	4条规定	相关名词释义与其他附则

中华人民共和国主席令

第五十三号

《中华人民共和国网络安全法》已由中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议于2016年11月7日通过，现予公布，自**2017年6月1日**起施行。

中华人民共和国主席 习近平

2016年11月7日

关键名词含义及解读

网络安全法所做的用语注释

网络安全

含义

是指通过采取必要措施，防范对网络的攻击、侵入、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，以及保障网络数据的完整性、保密性、可用性的能力。

解读

网络安全能力，通常包括：

- 基础设施的安全能力；
- 信息系统的安全能力；
- 信息自身的安全能力；
- 信息利用的安全能力。

} 数据安全

网络运营者

含义

是指网络的所有者、管理者和网络服务提供者。

解读

网络运营者，通常包括：

- 网络接入服务提供者（ISP）；
- 网络内容服务提供者（ICP）。

网络安全责任主体，通常包括：

- 网络的所有者；
- 网络的管理者；
- 网络的服务提供者；

个人信息

含义

是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

解读

个人信息不同于个人隐私，通常具有更强的商业性，主要特征包括：

- 具有可识别性，是指可直接识别确定特定个人身份的信息；
- 具有相对性，是指可关联或组成识别特定个人身份的信息。

所涉及的关键相关方和职责

国家

完善国家网络安全战略和方针、鼓励网络安全技术创新和应用，支持培养网络安全人才，建立保障体系，提高保护能力
推进国际交流合作

省级人民政府

网络安全风险监测评估，网络安全风险预警发布，履行网络安全监督管理职责；
扶持网络安全技术产业，支持和推广网络安全研究、产品和服务，保护知识产权，组织宣传教育

国家网信部门

负责统筹协调网络安全工作和相关监督管理工作

网络运营者

接受政府和社会监督，承担社会责任
按照等保要求，履行安全保护义务，防止网络数据泄露或者被窃取、篡改，维护网络数据的完整性、保密性和可用性
提供对犯罪活动调查的技术支持和协助

行业组织

健全行业的网络安全保护规范和机制，加强对网络风险的分析评估，定期进行风险警示，协助应对安全风险
加强行业自律，促进行业健康发展

标准化行政主管部门

负责组织制定并适时修订有关网络安全管理以及网络产品、服务和运行安全的国家标准、行业标准

电信主管部门

职责范围内负责网络安全保护和监督管理工作

公安部门

各自职责范围内负责网络安全保护和监督管理工作

处罚权

强化了相关组织的监管互动

网信办

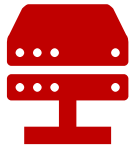
网络与信息安全信息通报中心

网络与信息安全应急事务中心

国家计算机网络应急技术处理协调中心

.....

与监管互动
将常态化



网络安全
事件汇报

企业合规
自我检查

主动参与行
业标准制定过程

监管机构

国务院

工信部

国资委

央行

银监会

保监会

证监会

税务局

工商局

第三章-网络运行安全的解读

关键信息基础设施（CII）
Critical Information Infrastructure

网络运行安全

一般规定

- 网络安全等级保护制度
- 产品和服务提供者的安全义务
- 关键及专用产品的认证检测
- 用户身份管理
- 应急处置措施
- 安全服务活动的规范
- 禁止危害的行为
- 技术支持和协助义务
- 安全风险的合作应对
- 执法信息用途限制

重点工作

- 制度、人员责任
- 防病毒和网络入侵
- 网络事件应急预案
- 服务提供实名制
- 网络监测和日志
- 数据分类、备份和加密
- 网络设备与产品
- 产品、服务需符合 标准

CII运行安全

- CII保护制度
- CII保护工作部门职责
- CII建设安全要求
- CII运营者的安全保护义务
- CII采购的国家安全审查
- CII采购的安全保密义务
- CII数据的境内存储和对外提供
- CII的定期安全检测评估
- CII保护的统筹协作机制

重点工作

- 制度、人员责任
- 防病毒和网络入侵
- 网络事件应急预案
- 至少每年安全评估
- 数据分类、备份加密
- 服务提供实名制
- 产品、服务需符合标准
- 网络监测和日志
- 跨境数据传输评估
- 应急预案并定期演练
- 重要数据境内存储
- 网络设备与产品
- 定期培训考核
- 保密协议
- 采购产品与服务安 全审查
- 系统与数据容灾备份

关于网络运营者视角的解读

相关条款

第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改；

第二十四条 网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。

第二十五条 网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

第二十八条 网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。

关于网络产品和服务者视角的解读

相关条款

第二十二条 网络产品、服务应当符合相关国家标准的强制性要求。

网络产品、服务的提供者不得设置恶意程序；　　发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。

网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

第二十六条 开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。

第二十三条 网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。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，并推动安全认证和安全检测结果互认，避免重复认证、检测。

关于相关组织视角的解读

相关条款

第二十四条 ……国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认。

第二十九条 国家支持网络运营者之间在网络安全信息收集、分析、通报和应急处置等方面进行合作，提高网络运营者的安全保障能力。

有关行业组织建立健全本行业的网络安全保护规范和协作机制，加强对网络安全风险的分析评估，定期向会员进行风险警示，支持、协助会员应对网络安全风险。

第三十条 网信部门和有关部门在履行网络安全保护职责中获取的信息，只能用于维护网络安全的需要，不得用于其他用途。

关于个人与组织视角的解读

相关条款

第二十七条 任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；

不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；（与刑法衔接）

明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。（与刑法衔接）

关于运营者的网络安全等级保护

GB/T 22239-2008
信息安全技术 信息系统
安全等级保护基本要求

GB/T 22239.1-2017 信息安全技术 网络安全等级保护基本要求 第1部分 安全通用要求

+

GB/T 22239.2-2017 信息安全技术 网络安全等级保护基本要求 第2部分 云计算安全扩展要求

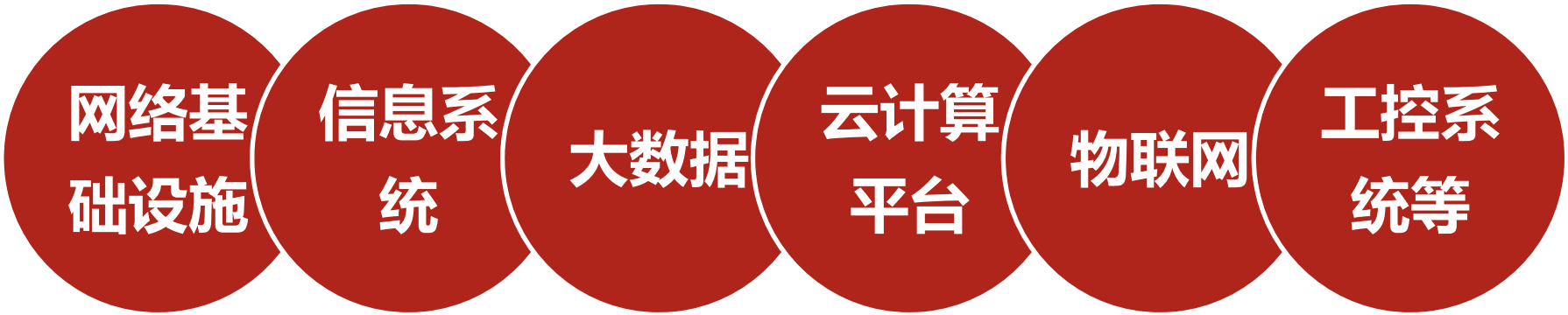
GB/T 22239.3-2017 信息安全技术 网络安全等级保护基本要求 第3部分 移动互联安全扩展要求

GB/T 22239.4-2017 信息安全技术 网络安全等级保护基本要求 第4部分 物联网安全扩展要求

GB/T 22239.5-2017 信息安全技术 网络安全等级保护基本要求 第5部分 工业控制安全扩展要求

GB/T 22239.6-2017 信息安全技术 网络安全等级保护基本要求 第6部分 大数据安全扩展要求

网络安全等级保护——等级划分



重要程度

危害程度

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

网络安全等级保护——等级划分

技术类安全要求与提供的技术安全机制有关，主要通过部署软硬件并正确的配置其安全功能来实现

管理类安全要求与各种角色参与的活动有关，主要通过控制各种角色的活动，从政策、制度、规范、流程以及记录等方面做出规定来实现

技术要求

+

管理要求

安全保护能力

第一级:用户自主保护级

第二级:系统审计保护级

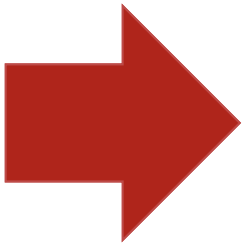
第三级:安全标记保护级

第四级:结构化保护级

第五级:访问验证保护级

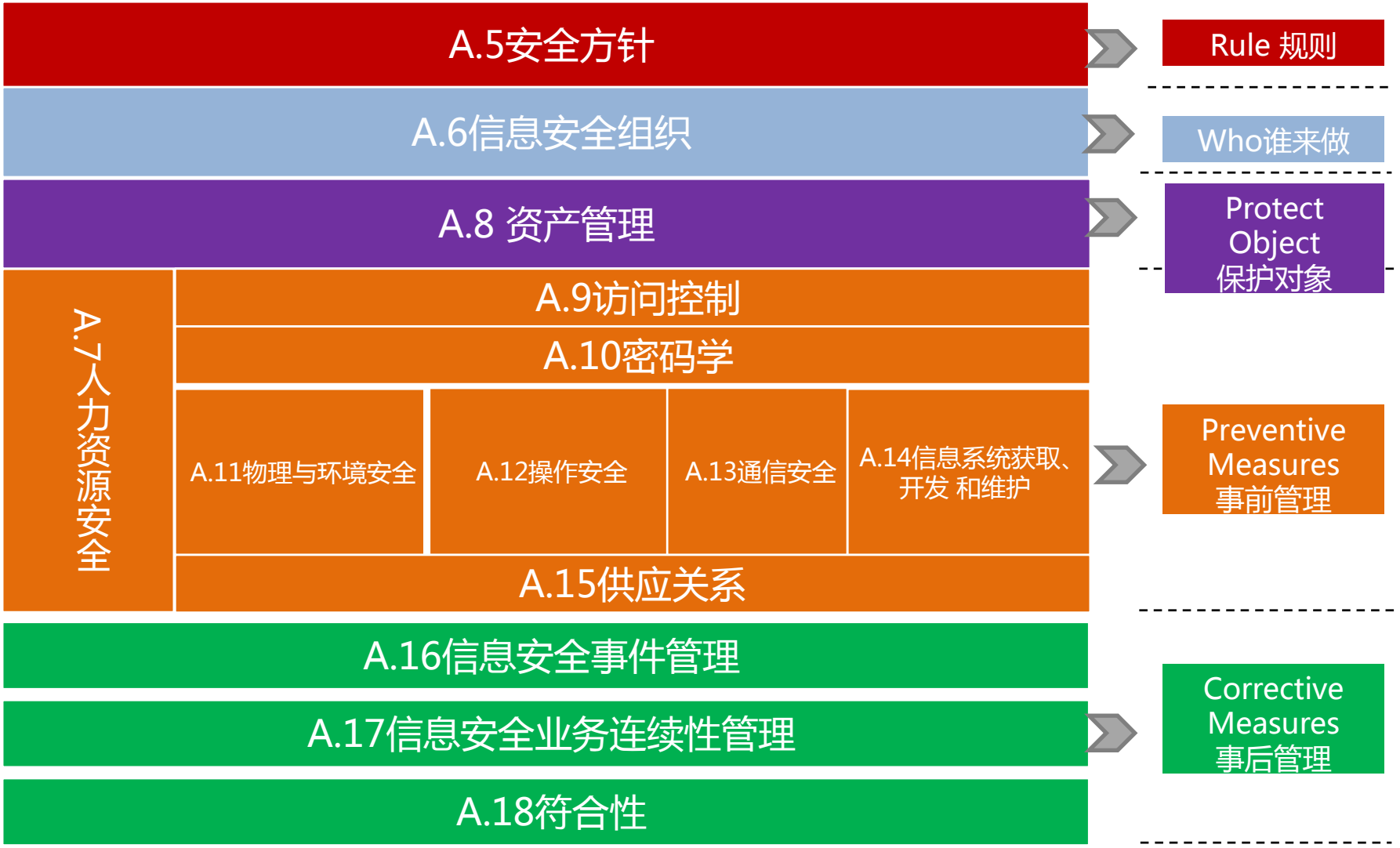
网络安全等级保护——安全控制领域差异

旧版	
技术要求	物理安全
	网络安全
	主机安全
	应用安全
	数据安全及备份恢复
管理要求	安全管理制度
	安全管理机构
	人员安全管理
	系统建设管理
	系统运维管理



新版	
物理和环境安全	技术要求
网络和通信安全	
设备和计算安全	
应用和数据安全	
安全策略和管理制度	管理要求
安全管理机构和人员	
安全建设管理	
安全运维管理	

关于运营者的安全管理体系

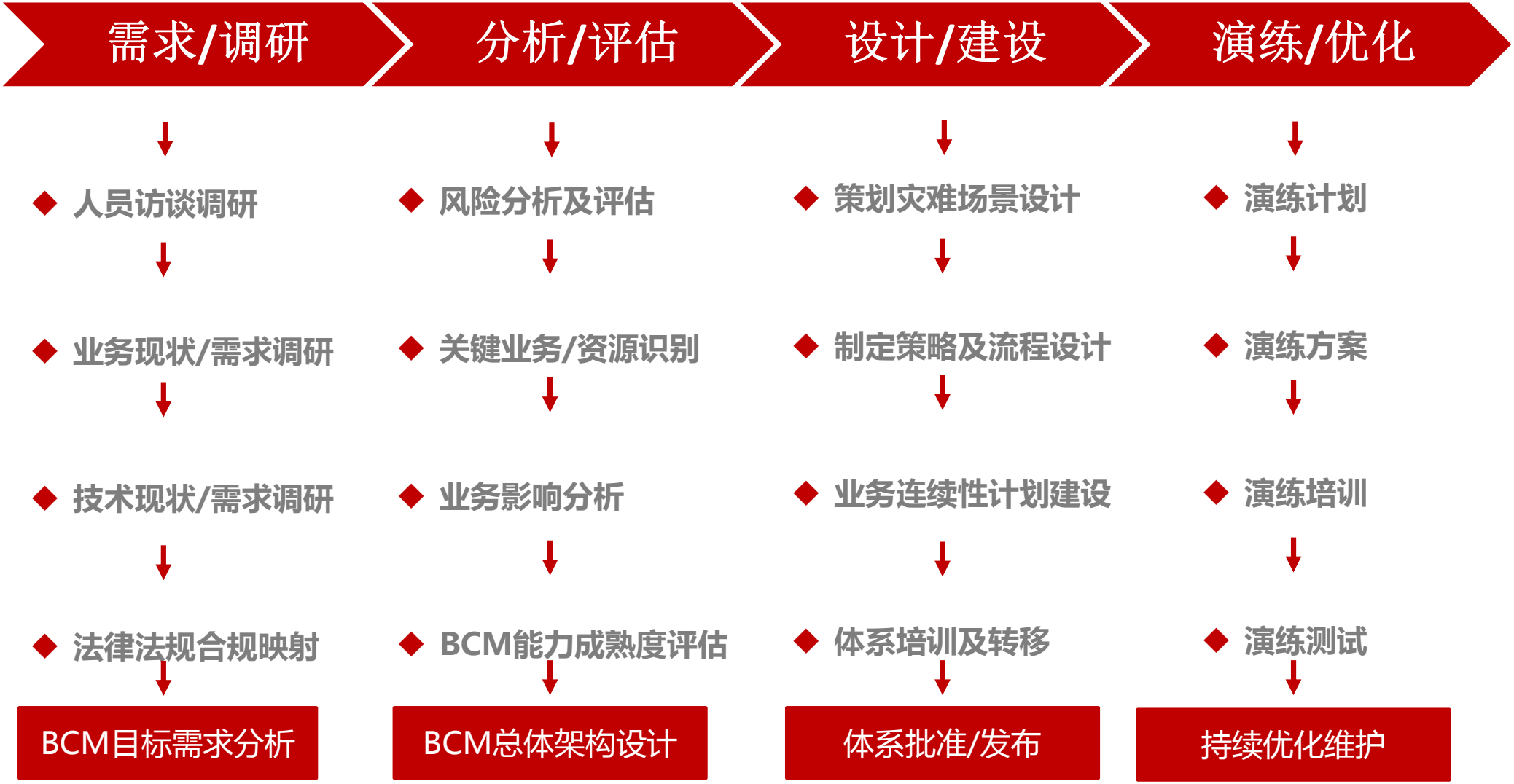


建议参考《ISO27001：2013 信息安全管理标准》

关于运营者的应急管理-应急管理架构

建议参考《ISO22301 业务连续性管理标准》

关于运营者的应急管理-风险分析架构



关于CII个人信息和重要数据的解读

- 数据本地化
  - 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。
  - 因业务需要，确需向境外提供的，应当进行安全评估；法律、行政法规另有规定的，依照其规定。

- 个人信息和重要数据应境内存储，出境前自行评估：

（一）数据处境的必要性；

（二）涉及个人信息情况，包括个人信息的数量、范围、类型、敏感程度，以及个人信息主题是否同意其个人信息处境等；

（三）涉及重要数据情况，包括重要数据的数量、范围、类型机器敏感程度等；

（四）数据接收方的安全保护措施、能力和水平，以及所在国家和地区的网络安全环境等；

（五）数据出境及再转移后被泄露、毁损、篡改、滥用等风险；

（六）数据出境及出境数据汇聚可能对国家安全、社会公共利益、个人合法利益带来的风险；

（七）其他需要评估的重要事项。

- 其它规定
  - 下列数据在其它法律里有本地化要求：国家秘密和国家安全数据、征信数据、个人金融信息、地图数据、网络出版服务所需的必要的技术设备、网约车相关数据和信息。

关于CII个人信息和重要数据的解读

- 以下情形出境数据应报请行业主管或监管部门评估：

（一）含有或累计含有50万人以上的个人信息；

（二）数据量超过1000GB；

（三）包含核设施、化学生物、国防军工、人口健康等领域数据，大型工程活动、海洋环境以及敏感地理信息数据等；

（四）包含关键信息基础设施的系统漏洞、安全防护等网络安全信息；

（五）关键信息基础设施运营者向境外提供个人信息和重要数据；

（六）其他可能影响国家安全和社会公共利益，行业主管或监管部门认为应该评估。

（七）行业主管或监管部门不明确的，由国家网信部门组织评估。

- 以下情况之一的，数据不得出境：

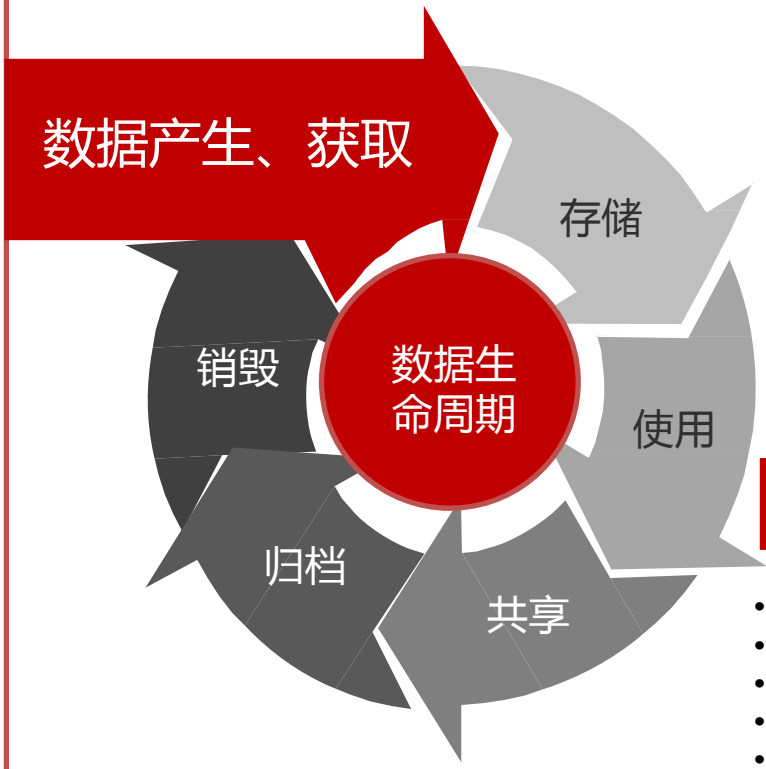
（一）个人信息出境未经个人信息主体同意，或可能侵害个人利益；

（二）数据出境给国家政治、经济、科技、国防等安全带来风险，可能影响国家安全、损害社会公共利益；

（三）其他经国家网信部门、公安部门、安全部门等有关部门认定不能出境的。

关于运营者的数据管理-数据识别和分析

网络运营者建立以数据分类分级为核心，数据生命周期为切入的，系统性数据安全管理框架。

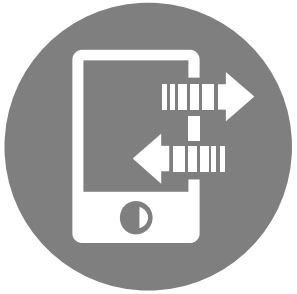


数据生成

- 数据分类
- 数据分级定义
- 数据质量
- 数据服务
- 数据流图(盘点)

存储与使用

- 数据使用安全标准
- 数据媒介管理
- 数据泄漏保护
- 数据库活动监控
- 数据屏蔽
- 数据加密



数据共享

- 数据传输安全标准
- 数据存储媒介
- 数字版权管理
- 数据访问管理

归档与销毁

- 数据归档安全标准
- 数据销毁安全标准
- 数据备份及恢复

数据资产清单

关于运营者的数据管理-数据管理策略

1 业务分类、数据分类

识别数据范围

业务驱动，优先级排序、定义重要数据分类包括数据项、数据子项、甚至数据字段，并定义对应的安全保护级别

- 秘密级
- 限制级

维护数据场景

基于数据生命周 期，识别数据载 体在搜集、使用、 共享、传输、存 储、销毁的场景（岗位、系统、第三方等）。

- 外部公开级
- 内部使用级

2 风险评估 制定标准

基于场景风险评估

基于已识别的场景，识别评估潜在的安全风险，了解当前的管控现状。

- 风险评估
- 威胁程度
- 脆弱性

制定数据安全标准

制定不同级别数 据、在数据生命 周期需遵循的数 据安全管理要求， 包括人防和技防。

- 管理流程
- 管理措施
- 人员管理

3 技术落地应急演练

规划技术管控蓝图

基于风险评估结果，对照数据安全标准，制定未来技术措施实施路线图。

- 风险评估
- 威胁程度
- 脆弱性

制定数据泄露、紧急预案

对照网络安全安 全事件紧急预案， 制定数据泄露紧 急预案。

- 管理流程
- 管理措施

网络运行安全-CII范围及行业职责

➢ CII的基本范围

“国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业…实行重点保护”。国务院另行制定关键信息基础设施的具体范围和安全保护办法。

相关国家关键基础设施分类情况

美国	**16个领域**，通信、信息技术、化工、关键制造、应急服务、水利、核反应堆及材料和废弃物、商业设施、政府设施、运输系统、能源、金融服务、水及污水处理系统、医疗保健和公共卫生、国防工业基地、食品和农业
德国	**8个领域**，卫生健康、信息与通信、供水、能源供给、交通运输、银行、保险与股票交易、食品供应-《联邦信息技术安全法》
日本	**13个领域**，信息通信、金融、行政、医疗、供排水、电力、燃气、化学、信贷、石油、航空、铁路、物流-《关键信息基础设施保护基本政策》

➢ 负责CII安全保护工作部门的职责：

1.负责编制并组织实施本行业、本领域的关键信息基础设施安全规划；

2.指导和监督关键信息基础设施运行安全保护工作；

CII重点增强型法律责任义务解读

建设要求

业务运行稳定可靠，安全技术措施同步规划、同步建设、同步使用

安全保护

专门安全管理机构和安全管理负责人：背景审查、安全教育、培训、考核；容灾备份；应急预案、定期演练；

安全审查

2015年国家安全审查制度

采购网络产品和服务，如影响国家安全，应当通过国家安全审查

保密要求

采购服务和产品，签订安全保密协议，明确安全和保密义务与责任。

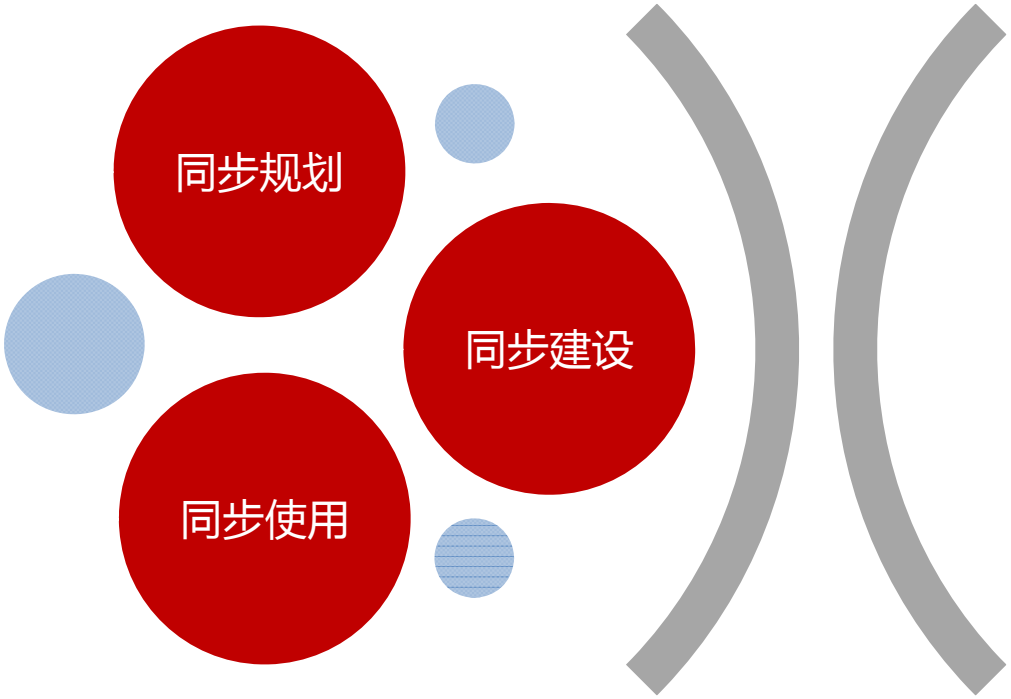
数据存储

个人信息和重要数据应当在境内存储；数据出境需进行评估

检测评估

每年至少进行一次检测评估，报送检测评估情况和改进措施

CII建设运营者的“三同时”解读



- 建设项目的设计单位在编制项目设计文件时，应当按照规定编制安全技术措施的设计文件；
- 关键信息基础设施的运营者在编制建设项目投资计划时，应当将安全技术措施所需投资一并纳入预算；
- 关键信息基础设施的运营者应当要求施工单位严格按照安全技术措施的设计要求施工；
- 在建设项目验收时，应当对安全技术措施进行调试、检测和验收；
- 安全技术措施应当与主体工程同时投入使用；

关于网络产品和服务安全审查的解读

- 网络安全重点审查网络产品和服务的安全性、可控性：

（一）产品和服务自身的安全风险，以及被非法控制、干扰和中断运行的风险；

（二）产品及关键部件生产、测试、交付、技术支持过程中的供应链安全风险；

（三）产品和服务提供者利用提供产品和服务的便利条件非法收集、存储、处理、使用用户相关信息的风险；

（四）产品和服务提供者利用用户对产品和服务的依赖，损害网络安全和用户利益的风险；

（五）其他可能危害国家安全的风险。

第四章 网络信息安全—个人信息保护

- **用户**：自然人、法人和其它组织
- **用户信息范围**：个人信息、隐私和法人和其他组织的商业秘密。
  - **用户信息**：引入了“用户信息”的概念，可以理解为在用户使用产品或服务过程中收集的信息构成用户信息，包括IP地址、GPS、用户名和密码、上网时间、Cookie信息等。
  - **个人信息**：个人信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

我国法律

- 《关于维护互联网安全的决定》
- 《关于加强网络信息保护的决定》
- 《消费者权益保护法》
- 刑法修正案（九）
- 《电信和互联网用户个人信息保护规定》
- ……

相关国家

- 经济合作与发展组织-《隐私保护和个人数据跨国流通指南》
- 联合国-《自动化资料档案中个人资料处理准则》
- 美国-《隐私权法案》
- 日本-《个人信息保护法》
- 欧盟-《通用数据保护条例》

与个人信息的相关条款

（第四十九条）网络运营者应当**建立网络信息安全投诉、举报制度，公布投诉、举报方式等信息**，及时受理并处理有关网络信 息安全的投诉与举报

（第四十一条）网络运营者收集、使用个人信息，**应公开搜集、使用规则，明示搜集、使用信息的目的、方式和范围**并经被搜集者同意

（第四十一条）网络运营者收集、使用个人信息，应当遵循**合法、正当、必要原则；不得搜集**与其服务提供**无关**的个人信息

（第四十二条）**未经被**搜集者**同意，不得向他人提供个人信息，但是**经过处 理无法识别特定个人且不能复原的除外；
（第四十四条）不得非法出售或非法向他人提供个人信息

（第四十一条）网络运 营者收集、使用个人信息，应经**被搜集者同意**；
（第四十二条）**未经**被搜集者**同意，不得向他人提供**个人信息

（第四十二条）网络运营者不得**泄露、篡改、毁损**其搜集的个人信息

（第四十二条）网络运营者不得**泄露、篡改、毁损**其搜集的个人信息

（第四十三条）个人发现网络运营者违反法律、行政法规的规定或**双方约定** 收集、使用个人信息的，**有权要求删除**其个人信息，发现有错误的**有权要求网络运营中更正**

（第四十条）网络运营者对其搜集的用户信息严格保密，**建立健全用户信息保护制度**

关于个人信息保护的限制和义务

- 个人信息保护：与以往法律法规相比，增加了删除权和更正权：
  - 应当遵守本法和有关法律、行政法规的规定；
  - 收集、使用个人信息：应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意；
  - 不得泄露、篡改、毁损其收集的个人信息：1）采取技术措施和其他必要措施保护；2）若泄漏，立即采取补救措施，告知用户并向有关主管部门报告；
  - 未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。
  - 个人信息主体拥有删除权和更正权；
  - 不得非法获取、窃取，不得非法出售、非法向他人提供；
  - 网络运营者应当建立网络信息安全投诉、举报制度，公布投诉、举报方式。

欧盟关于通用数据保护原则

合法、正当、透明原则；特定、明确目的原则；目的是当、相关、限制原则；

关于个人信息删除权和更政权的解读

使用删除权的情形

- 收集、使用行为不具备合法性，如非法收集、超出法定或约定范围；
- 收集、使用个人信息的目的消失，是对个人信息的保存及处理、利用失去了必要性、正当性；
- 约定的收集、使用、保存个人信息的期限届满。

使用更正权的情形

- 个人信息收集、存储使用过程中，个人信息不完整或不准确，有权要求及时改正、补充的权利

网络信息安全—网络行为的解读

➢ 网络行为要求

- 第四十四条 任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。
- 第四十六条 任何个人和组织应当对其使用网络的行为负责，不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。
- 第四十七条 网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

关于利用网络发布犯罪或恶意信息的的解读

- 设立网络、通讯群组或者通过网络发布信息，目的是为实施违法犯罪而与做准备的。
- 行为人设立网站、通讯群租或者发布网络信息，主要是为了实施诈骗、传授犯罪方法、制作或者销售违禁品、管制物品等违法活动

监测预警与应急处理

➢ 国家及主管部门

- 建立网络安全监测预警和信息通报制度。按照规定统一发布网络安全监测预警信息
- 关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息
- 国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练
- 网络安全事件发生的风险增大时，省级以上人民政府有关部门应当按照规定的权限和程序，并根据网络安全风险的特点和可能造成的危害：检测、评估、预警、补救措施
- 发生网络安全事件，应当立即启动网络安全事件应急预案，对网络安全事件进行调查和评估，要求网络运营者采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时向社会发布与公众有关的警示信息

监测预警与应急处理

- 国家及有关部门

◆ 省级以上人民政府有关部门在履行网络安全监督管理职责中，发现网络存在较大安全风险或者发生安全事件的，可以按照规定的权限和程序对该网络的运营者的法定代表人或者主要负责人进行约谈。

◆ 因网络安全事件，发生突发事件或者生产安全事故的，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、行政法规的规定处置。

◆ 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，经国务院决定或者批准，可以在特定区域对网络通信采取限制等临时措施。

- 网络运营者

◆ 存在较大安全风险或发生安全事件：网络运营者应当按照要求采取措施，进行处置、整改，消除隐患，并及时公布警示信息。

◆ 与《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》等有关法律作衔接。

法律责任

➢ 行政处罚

- ◆ 责令**改正、警告、罚款**，
- ◆ 责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员等进行罚款等；
- ◆ 有关机关还可以把违法行为**记录到信用档案**。
- ◆ 对于“非法入侵”等，法律还建立了**职业禁入**的制度。

➢ 民事责任

- ◆ 违法《网络安全法》的行为给他人造成损失的，网络运营者应当承担相应的民事责任。

➢ 治安管理处罚/刑事责任

- ◆ 违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

处罚对象	处罚类型	所涉及处罚和金额	所涉及处罚行为
网络运营者	经济	最高5万	不履行本法第二十一条、第二十五条规定的网络安全保护义务
			违反本法第二十四条第一款规定（未要求用户提供真实身份、或者不提供真实身份）
		最高10万	违反本法第二十四条第一款规定（未要求用户提供真实身份、或者不提供真实身份）
			违反本法第四十七条规定（对法律、行政法规禁止发布或者传输的信息未停止采取处置措施）
		最高50万	违反本法第四十七条规定（对法律、行政法规禁止发布或者传输的信息未停止采取处置措施）
			1）不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息采取处置措施； 2）拒绝阻碍有关部门依法实施监督检查； 3）拒不向公安机关、国家安全机关提供（技术支持和协助）
			不履行本法第四十八条第二款规定（电子信息发送服务提供者、应用软件下载服务提供者）安全管理义务
		最高100万	违反本法第二十二条第三款、第四十一条到四十三条规定（侵害个人信息）
			违反本法第四十四条规定，（窃取、非法获取、出售或非法向他人提供个人信息）
直接负责人	经济	最高5万	不履行本法第二十一条、第二十五条规定的网络安全保护义务
		最高10万	违反本法第二十二条第三款、第四十一条到四十三条规定（侵害个人信息）
			1）不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息采取处置措施； 2）拒绝阻碍有关部门依法实施监督检查； 3）拒不向公安机关、国家安全机关提供（技术支持和协助）
网络运营者	行政	暂停相关业务、停业整顿、关闭网站、吊销相关许可、营业执照	违反本法第二十四条第一款规定（未要求用户提供真实身份、或者不提供真实身份）
			违反本法第四十七条规定（对法律、行政法规禁止发布或者传输的信息未停止采取处置措施）
			违反本法第二十二条第三款、第四十一条到四十三条规定（侵害个人信息）

处罚对象	处罚类型	所涉及处罚和金额	所涉及处罚行为
关键信息基础设施运营者	经济	最高50万	违反本法第三十七条规定，（境外存储网络数据、或者向境外提供网络数据）
		最高100万	不履行本法第三十三条、第三十四条、三十六条、三十八条规定的网络安全保护义务
直接负责人	经济	最高10万	不履行本法第三十三条、第三十四条、三十六条、三十八条规定的网络安全保护义务
			违反本法第三十七条规定，（境外存储网络数据、或者向境外提供网络数据）
			违反本法第三十五条规定，（未经安全审查或者未通过的网络产品和服务）
关键信息基础设施运营者	行政	暂停相关业务、停业整顿、关闭网站、吊销相关许可、营业执照	违反本法第二十二条第三款、第四十一条到四十三条规定（侵害个人信息）
			违反本法第三十五条规定，（未经安全审查或者未通过的网络产品和服务）
			违反本法第三十七条规定，（境外存储网络数据、或者向境外提供网络数据）

处罚对象	处罚类型	所涉及处罚和金额	所涉及处罚行为
个人、组织	经济	最高10万	违反本法第二十六条规定（网络安全认证、检测、风险评估等活动，或者发布系统漏洞、计算机病毒、网络攻击、入侵等）
			违反本法第四十六条规定，（违法犯罪活动的网站、通讯群组，或利用网络发布犯罪活动的信息）
		最高50万	违反本法第二十二条第一款、第二款和第四十八条第一款规定行为之一
			违反本法第四十六条规定，（违法犯罪活动的网站、通讯群组，或利用网络发布犯罪活动的信息）
			违反本法第二十七条规定（危害网络安全活动的程序、工具或者为他人提供技术支持、广告推广支付结算等）
		最高100万	违反本法第二十七条规定（危害网络安全活动的程序、工具或者为他人提供技术支持、广告推广支付结算等）
直接负责人	经济	最高5万	违反本法第二十六条规定（网络安全认证、检测、风险评估等活动，或者发布系统漏洞、计算机病毒、网络攻击、入侵等）
		最高10万	违反本法第二十二条第一款、第二款和第四十八条第一款规定行为之一
		最高50万	违反本法第四十六条规定，（前款行为）
个人、组织	行政	暂停相关业务、停业整顿、关闭网站、吊销相关许可、营业执照	违反本法第二十六条规定（网络安全认证、检测、风险评估等活动，或者发布系统漏洞、计算机病毒、网络攻击、入侵等）
个人、组织	法律	五年	违反本法第二十七条规定，受到治安管理处罚人员不得从事网络安全管理和网络运营关键岗位工作
		终身	违反本法第二十七条规定，受到刑事处罚人员不得从事网络安全管理和网络运营关键岗位工作
		拘留（最高5/日）尚不构成犯罪	违反本法第二十七条规定（危害网络安全活动的程序、工具或者为他人提供技术支持、广告推广支付结算等）
			违反本法第四十六条规定，（违法犯罪活动的网站、通讯群组，或利用网络发布犯罪活动的信息）
		拘留（最高15/日）情节较重	违反本法第四十六条规定，（违法犯罪活动的网站、通讯群组，或利用网络发布犯罪活动的信息）
			违反本法第二十七条规定（危害网络安全活动的程序、工具或者为他人提供技术支持、广告推广支付结算等）
		记录信用档案、公示	违法本法规定
		承担民事责任	违反本法规定，给他人造成损害的
		治安管理处罚	违反本法规定，造成治安管理行为
		追究刑事责任	违反本法规定，构成犯罪

处罚对象	处罚类型	所涉及处罚和金额	所涉及处罚行为
网络产品或者服务的提供者	经济	最高100万	违反本法第二十二条第三款、第四十一条到四十三条规定（侵害个人信息
			违反本法第四十四条规定，（窃取、非法获取、出售或非法向他人提供个人信息）
直接负责人	经济	最高10万	违反本法第二十二条第三款、第四十一条到四十三条规定（侵害个人信息
网络产品或者服务的提供者	行政	暂停相关业务、停业整顿、关闭网站、吊销相关许可、营业执照	违反本法第二十二条第三款、第四十一条到四十三条规定（侵害个人信息

处罚对象	处罚类型	所涉及处罚和金额	所涉及处罚行为
电子信息发送服务提供者	经济	最高50万	不履行本法第四十八条第二款规定的安全管理义务
直接负责人	经济	最高10万	不履行本法第四十八条第二款规定的安全管理义务
电子信息发送服务提供者	行政	暂停相关业务、停业整顿、关闭网站、吊销相关许可、营业执照	不履行本法第四十八条第二款规定的安全管理义务

处罚对象	处罚类型	所涉及处罚和金额	所涉及处罚行为
应用软件下载服务提供者	经济	最高50万	不履行本法第四十八条第二款规定的安全管理义务
直接负责人	经济	最高10万	不履行本法第四十八条第二款规定的安全管理义务
应用软件下载服务提供者	行政	暂停相关业务、停业整顿、关闭网站、吊销相关许可、营业执照	不履行本法第四十八条第二款规定的安全管理义务

处罚对象	处罚类型	所涉及处罚和金额	所涉及处罚行为
直接负责人	法律	依法处分	不履行本法规定的网络安全保护义务
国家机关政务网络运营者	行政	责令改正	不履行本法规定的网络安全保护义务

处罚对象	处罚类型	所涉及处罚和金额	所涉及处罚行为
直接负责人	法律	依法处分	违反本法第三十条规定（网络安全保护职责获取的信息用于其它用途）
网信部门和有关部门（工作人员）			玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的

处罚对象	处罚类型	所涉及处罚和金额	所涉及处罚行为
境外机构（组织、个人）	经济	冻结财产	攻击、侵入、干扰、破坏、危害中华人民共和国关键信息基础设施活动
	法律	追究法律责任	攻击、侵入、干扰、破坏、危害中华人民共和国关键信息基础设施活动