第一章　网络信息安全基础
第三节　网络空间安全法律法规及标准 - 网络安全法

主讲人：李建华　张全海
网络空间安全技术研究院

2024 年 9 月

上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

目 录

《网络安全法》立法背景

应对网络安全威胁已是全球性问题，国际网络安全的法治环境正发生巨大变革，美欧等网络强国纷纷建立全方位、立体化、更具弹性与前瞻性的网络安全立法体系，**网络安全立法已演变为全球范围内的国家主权与利益的斗争，有法可依成为了谈判与对抗的必要条件**。

- 国际背景
- 国内背景

国际背景

合作与共赢

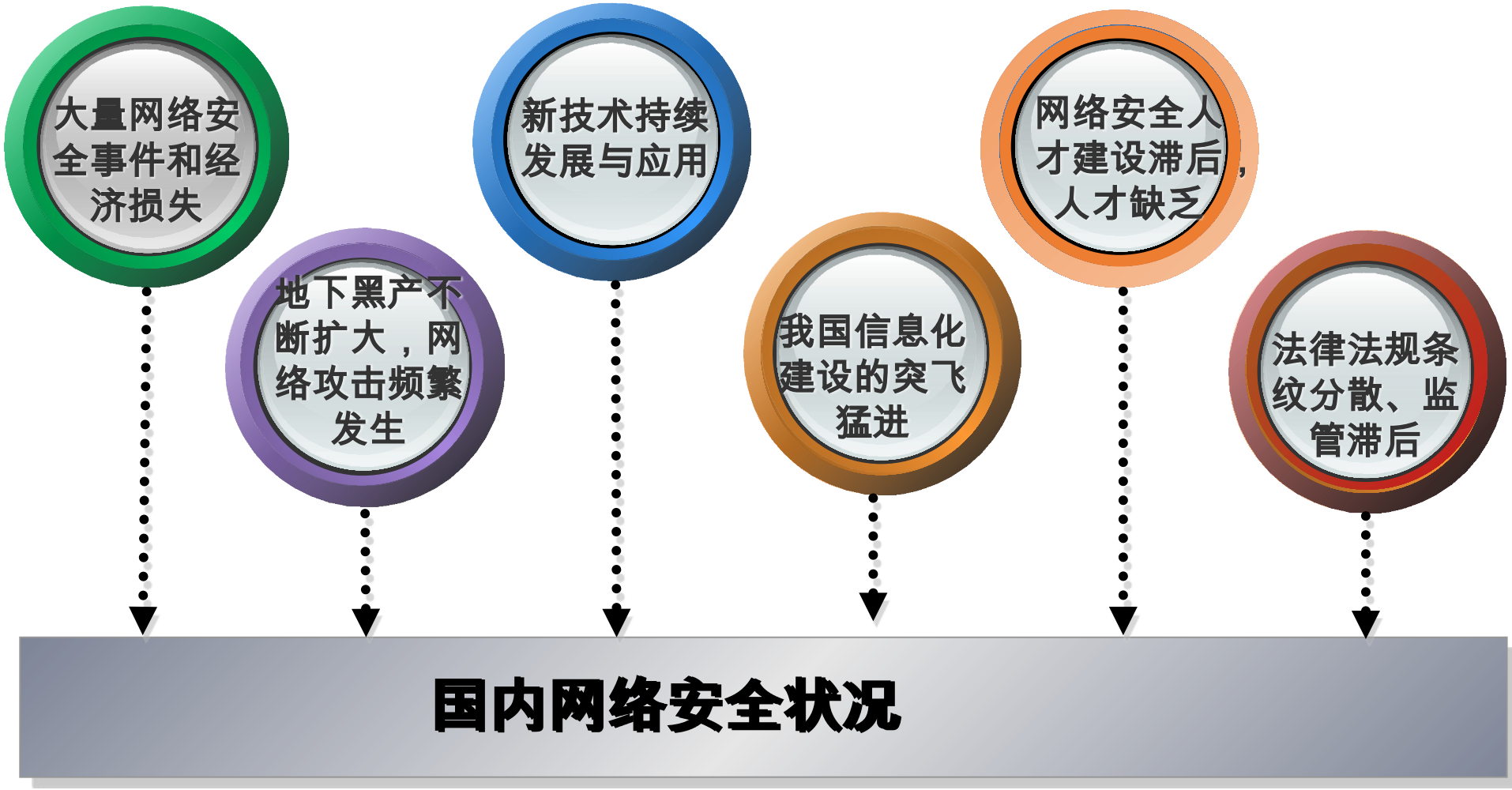
- 2015 年 9 月，习主席访美提出“打造中美合作亮点，让网络空间更好地造福两国人民和世界人民”
- 2015 年 12 月，中美达成了《打击网络犯罪及相关事项指导原则》
- 2015 年以来，中英、中俄、中德先后签署了合作协议。中英，中德之间开展高级别对话深化网络犯罪国际合作。
- 2016 年 11 月，习主席在第二届世界互联网大会（浙江省乌镇）系统论述了“网络空间命运共同体”的理念，重点提出“四点原则”和“五个主张”的中国方案。

国际背景

冲突与对抗

- 网络冲突和攻击成为国家间对抗的主要形式。
- 网络空间战略和政策升级调整
- 注重安全保障与攻击能力双向提升
- 加强对数据资源跨境传输的管控
- 2015 年以来，国家行为体实施的大规模网络监控和网络攻击造成了国家间的严重不信任情绪，对国际局势的稳定带来不良影响。

国内背景


大量网络安全事件和经济损失
地下黑产不断扩大，网络攻击频繁发生
新技术持续发展与应用
我国信息化建设的突飞猛进
网络安全人才建设滞后，人才缺乏
法律法规条纹分散、监管滞后
国内网络安全状况

国内网络安全事件

- 2014 年 3 月 22 日，携程网安全支付日志下载漏洞被黑客利用，导致大量用户银行卡信息泄露；2015 年 5 月 28 日，携程网站和 APP 全线瘫痪，从瘫痪到修复，携程“宕机”近 12 小时，创下国内互联网公司系统瘫痪新纪录。
- 2015 年 4 月 22 日，重庆、上海、沈阳、贵州等超 30 个省市卫生和社保系统出现大量高危漏洞，数千万用户的社保信息被泄露，包括个人身份证、社保参保信息、财务、薪酬、房屋等敏感信息。
- 2015 年 6 月 中石化“内鬼”事件，系统内部技术人员，通过提供给中石化华东公司的 SCADA 系统（油管监控系统）对应开发了一套病毒程序，病毒爆发导致系统无法运行。

国外网络安全事件

- 2011 年 4 月 12 日，韩国最大农协银行遭遇黑客，导致客户三天无法提款、转账、使用信用卡，大约 540 万名信用卡客户的交易记录被删除。
- 2015 年 12 月 3 日，乌克兰电网遭黑客攻击，黑客使用后门程序 BlackEnery(黑暗力量) 攻击了在发电站和多家能源公司，在寒冷冬天数百万家庭供电被迫中断。
- 2015 年 12 月 31 日，由于严重的“分布式拒绝服务”攻击 (DDOS) ，英国广播公司 (BBC) 网站和 iPlayer 服务被迫下线。该攻击导致网站瘫痪数小时。
- 比特币勒索病毒”在全球爆发，至少有 150 个国家受到网络病毒攻击，大量组织机构受害严重包括金融、能源、医疗、教育等行业。中国部分 Windows 操作系统用户遭受感染，校园网用户首当其冲，大量实验室数据和毕业设计被锁定加密。

网络安全事件特点

安全事件特点

目标明确

信息安全事件大多为敌对国家或利益集团为达到某种目的而发起的网络攻击。往往是向指定的目标发起特定的网络攻击，具有极强的针对性。

隐蔽性强

攻击工业控制系统的病毒和黑客，异常熟悉工业控制系统的网络情况，攻击方法独特导致无法及时发现，具有极强的隐蔽能力，可以长时间隐藏于工业控制系统中。

破坏严重

电力、能源、金融等系统如果遭到破坏，轻则造成经济损，重则会造成人身伤亡，甚至会影响地区和国家的安定，乃至国家战略和重大计划的执行都会受到阻挠。

网络安全立法的需求

- 从国内外严峻的网络安全形势和国内法制基础来看，“棱镜门”事件暴露出维护国家数据主权、振兴民族产业的法律保障不足；
- 能源、交通、金融、电力等国家关键信息基础设施建设、管理法制不健全，信息安全技术研究和产品开发政策法律保障乏力，在发生重大、突发事件和紧急状态情况下，应急响应缺乏法律保障，应急预案、违法犯罪信息和安全测试等可以用于社会安全防范的信息难以共享，严重影响了快速反应能力、安全保障能力和统一调配能力。
- 面对严峻的网络安全形势，仅对原有法律的解释、修订或增补，难以把握好安全与发展之间的关系，不利于国家总体安全战略目标的实现，我国亟需制定综合性“网络领域基本法”，应当明确规定网络与信息安全的基线，为部门、地方的立法和政策的制定、调整和完善提供法律依据

国外网络安全立法状况

01

美国

2015 年美国发布了《 2015 年网络安全法案》
2017 年美国发布了《增强联邦政府网络与关键基础设施网络安全》行政令

俄罗斯

2016 年俄罗斯发布了《俄联邦信息安全学说》

02

日本

2014 年，发布了《网络安全基本法》

03

欧盟

2016 年，欧洲议会通过了《网络安全与信息指令》，
2018 年 5 月 25 日生效的欧盟《通用数据保护条例》（简称 GDPR ）

网络空间安全顶层设计

2014 年成立**中央网络安全和信息化领导小组**，将信息安全提升到国家战略高度，习近平亲自担任组长。 4 月 27 日，在中央网络安全和信息化领导小组第一次会议上讲话，指出：**没有网络安全就没有国家安全，没有信息化就没有现代化。建设网络强国，要有自己的技术，有过硬的技术；要有丰富全面的信息服务，繁荣发展的网络文化；要有良好的信息基础设施，形成实力雄厚的信息经济；要有高素质的网络安全和信息化人才队伍；要积极开展双边、多边的互联网国际交流合作。建设网络强国的战略部署要与“两个一百年”奋斗目标同步推进，向着网络基础设施基本普及、自主创新能力显著增强、信息经济全面发展、网络安全保障有力的目标不断前进。**

国家高度重视

国务院

2016 年 5 月 13 号，国务院发布《关于深化制造业与互联网融合发展的指导意见》（国发〔2016〕28 号）。《意见》明确指出“以建设制造业与互联网融合“双创”平台为抓手，发展智能制造……与互联网融合新模式，……**提高工业信息系统安全水平**……”

工信部

2016 年 11 月 3 号工信部下发《工业控制系统信息安全防护指南》，指南指出“工业控制系统应用企业应从**安全软件选择与管理、配置和补丁管理、边界安全防护、物理和环境安全防护、身份认证、远程访问安全、安全监测和应急预案演练、资产安全、数据安全、供应链管理、落实责任**十一个方面做好工控安全防护工作”。

网信办

2016 年 7 月全国范围关键信息基础设施网络安全检查工作启动，习近平总书记指出：“**金融、能源、电力、通信、制造**等领域是经济社会运行的神经中枢，是网络安全的重中之重，也是可能遭到重点攻击的目标”，要求“要全面**加强网络安全检查，摸清家底，认清风险，找出漏洞，通报结果，督促整改**”。

立法进程

2014 年 → 2015 年 → 2016 年 → 2017 年

筹划

- 2014 年上 半年，全国人大法工委组成工作专班，开展网络安全法 研究起草工作。
- 通过召开座谈会、论证会等多种方式听取意见
- 提出了网络安全立法的基本思路、制度框架和 草案初稿，形成了网络安全法草案

发展

- 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《中华人民共和国网络安全法》草案一审稿。
- 草案在中国人大网公布，向社会公开征求意见

确定

- 2016 年 6 月，第十二届全国人大常委会第二十一次会议审议《中华人民共和国网络安全法》草案二次审议稿，，向社会公开征求意见
- 2016 年 11 月，第十二届全国人大常委会第二十四次会议审议通过《中华人民共和国网络安全法》（ 154 票赞成，1 票弃权 ）

实施

2017 年 6 月 1 日起正式实施

上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

目 录

网络安全立法里程碑

- 如何应对网络安全威胁已是全球性问题，国际网络安全空间格局发生重大变化，国际网络安全的法治环境正经历变革，美欧等网络强国纷纷建立全方位、更立体、更具弹性与前瞻性的网络安全立法体系，网络安全立法演变为全球范围内的利益协调与国家主权斗争，有法可依成为谈判与对抗的必要条件。
- 《网络安全法》的出台具有里程碑式的意义。它是全面落实党的十八大和十八届三中、四中、五中、六中全会相关决策部署的重大举措，是我国第一部网络安全的专门性综合性立法，提出了应对网络安全挑战这一全球性问题的中国方案。
- 立法进程的快速推进，显示了党和国家对网络安全问题的高度重视，是我国网络安全法治建设的一个重大战略契机。
- 网络安全有法可依，信息安全行业将由合规性驱动过渡到合规性和强制性驱动并重。

服务与国家网络安全战略和网络强国建设

- **网络空间逐步成为世界主要国家展开竞争和战略博弈的新领域。**我国作为一个拥有大量网民并正在持续发展中的国家，不断感受到来自现存霸主美国的战略压力。这决定了网络空间成为我国国家利益的新边疆，确立网络空间行为准则和模式已是当务之急。

- 现代国家是法治国家，国家行为的规则由法律来决定。《网络安全法》中明确提出了有关国家网络空间安全战略和重要领域安全规划等问题的法律要求，这有助于实现推进中国在国家网络安全领域明晰战略意图，确立清晰目标，厘清行为准则，**不仅能够提升我国保障自身网络安全的能力，还有助于推进与其他国家和行为体就网络安全问题展开有效的战略博弈**。

助力网络空间治理，护航“互联网 +”

- 我国是名符其实的网络大国，但是现实的网络环境十分堪忧，网络诈骗层出不穷、网络入侵比比皆是、个人隐私肆意泄露。但此前其他关于网络信息安全的规定、大多分散在众多行政法规、规章和司法解释中，因此无法形成具有针对性、适用性和前瞻性的法律体系。
- 《网络安全法》将成为新的起点和转折点。公民个人信息保护进入正轨，网络暴力、网络谣言、网络欺诈等“毒瘤”生存的空间将被大大挤压，而“四有”中国好网民从道德自觉走向法律规范，用法律武器维护自己的合法权益。
- 国家网络空间的治理能力在法律的框架下将得到大幅度提升，营造出良好和谐的互联网环境，更为“互联网 +” 的长远发展保驾护航。“互联网 +” 必须带上“安全”才能走的更远。

构建我国首部网络空间管辖基本法

- 《网络安全法》属于国家基本法律，是网络安全法制体系的重要基础，规范了网络空间多元主体的责任义务，以法律的形式催生了一个维护国家主权、安全和发展利益的“命运共同体”。
- 《网络安全法》规定了信息安全法的总体目标和基本原则；规范网络社会中不同主体所享有的权力义务及其地位；建立网站身份认证制度，实施后台实名；建立网络信息保密制度，保护网络主体的隐私权；建立行政机关对网络信息安全的监管程序和制度，规定对网络信息安全犯罪的惩治和打击；规定具体的诉讼救济程序等等。
- 《网络安全法》的出台从根本上填补了我国综合性网络信息安全基本大法、核心的网络信息安全法和专门法律的三大空白。

提供维护国家网络主权的法律依据

- 一些西方主要国家为维护网络空间主权，很早就制定了法律法规，并将维护网络安全纳入国家安全战略，且形成了较为完备的网络安全法律体系。美国目前已有四十余部网络安全相关立法，又在指定《国家网络安全和关键基础设施法保护法》

- 我国在 2016 年 7 月推出了《国家安全法》，首次以法律的形式明确提出了“维护国家网络空间主权”。《网络安全法》是《国家安全法》在网络安全领域的体现和延伸，为我国维护网络主权、国家安全提供了最主要的法律依据。

在网络空间领域贯彻落实依法治国精神

- 十八届四中全会通过了《中共中央关于全面推进依法治国若干重大问题的决定》，为我国的国家治理体系和治理能力现代化指明了方向，也为网络空间治理提供了指南。

- 近年来互联网的飞速发展，许多监管、治理手段相对滞后，大都是根据问题进行后期补充。《网络安全法》则开启了依法治网的崭新局面，成为依法治国顶层设计下一项共建共享的路径实践。依法治网成为我国网络空间治理的主线和引领，依法治谋求网治的长治久安。

成为网络参与者普遍遵守的法律准则和依据

- 网络不是法外之地，《网络安全法》的执行，成为**各方参与互联网上的行为提供非常重要的准则**，所有参与者都要按照《网络安全法》的要求来规范自己的行为，同样所有网络行为主体所进行的活动，包括国家管理、公民个人参与、机构在网上的参与、电子商务等都要遵守。

- 《网络安全法》对**网络产品和服务提供者的安全义务**有了明确的规定，将**现行的安全认证和安全检测制度上升成为了法律**，强化了安全审查制度，通过这些规定，使得所有网络行为都有法可依，有法必依，任何个人利益触碰法律底线的行为都将受到法律的制裁。

上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

目 录

《网络安全法》概览

《网络安全法》共7章79条：

第一章 总则
第二章 网络安全支持与促进
第三章 网络运行安全
第四章 网络信息安全
第五章 监测预警与应急处置
第六章 法律责任
第七章 附则

《网络安全法》第二章至第五章对网络安全有关事项进行规定，勾勒了我国网络安全工作的轮廓：以关键信息基础设施保护为重心，强调落实运营者责任，注重保护个人权益，加强动态感知快速反应，以技术、产业、人才为保障，立体化地推进网络安全工作。

《中华人民共和国网络安全法》自 2017 年 6 月 1 日起施行，这在网络安全历史上具有里程碑意义。《网络安全法》的公布和施行，解决了我国网络安全“基本法”的问题，网络安全工作有了基础性的法律框架。不仅从法律上保障了广大人民群众在网络空间的利益，有效维护了国家网络空间主权和安全，而且还有利于信息技术的应用，有利于发挥互联网的巨大潜力。

网络主权是国家主权在网络空间的体现和延伸，网络主权原则是我国维护国家安全和利益、参与网络国际治理与合作所坚持的重要原则。

《网络安全法》概览

定位

- 是互联网领域、网络安全的基础性法律。
- 是党的十八大以来的又一部重要法律。

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

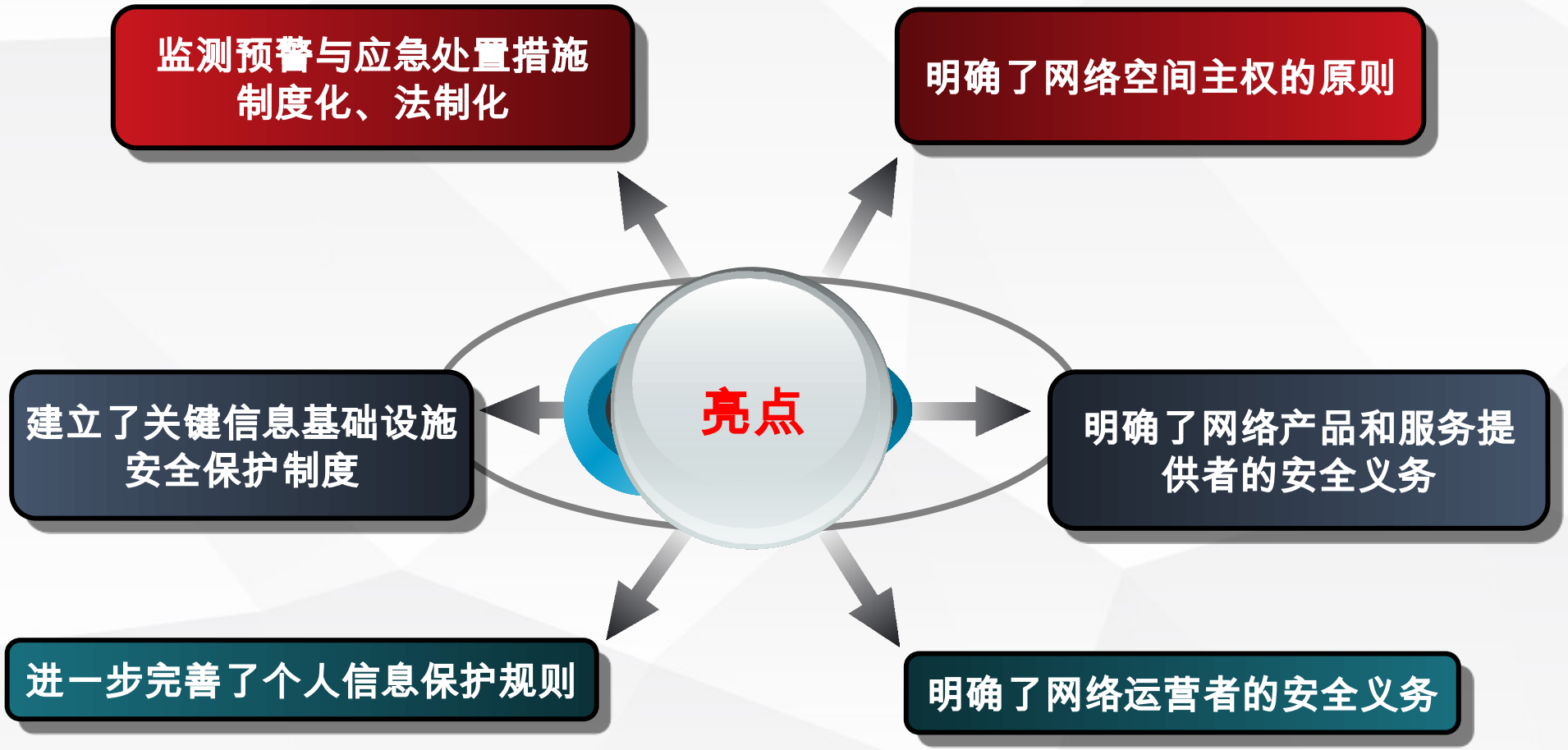
范围

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

总览

- 2016 年 11 月 7 日发布
- 2017 年 6 月 1 日起施行

《网络安全法》亮点


监测预警与应急处置措施制度化、法制化
明确了网络空间主权的原则
亮点
建立了关键信息基础设施安全保护制度
明确了网络产品和服务提供者的安全义务
进一步完善了个人信息保护规则
明确了网络运营者的安全义务

《网络安全法》亮点

全面性

具有全面性

全面和系统地**确立了各个主体**包括国家有关主管部门、网络运营者、网络使用者在网络安全保护方面的义务和责任；
确立了保障网络的**设备设施安全、网络运行安全、网络数据安全以及网络信息安全等**方面的基本制度。

针对性

具有针对性

从**我国的国情出发**，坚持问题的导向，总结实践经验，也借鉴了其他国家的一些做法，建立保障网络安全的各项制度，**重在管用，重在解决实际问题**

协调性

具有协调性

始终**坚持安全与发展并重**的原则，协调推进网络安全和发展，**注重保护网络主体的合法权益**，保障网络信息依法、有序、自由的流动，促进网络技术创新，最终实现**以安全促发展，以发展来促安全**的目的。

上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

目 录

《网络安全法》重要条款

* 第一章 总 则
第一章（共 14 条），主要描述制定网络安全法的目的和适用范围，保障网络安全的目标以及各部门、企业、个人所承担的责任义务，并强调将大力宣传普及，**加快配套制度建设，加强基础支撑力量建设**，确保网络安全法有效贯彻实施。

《网络安全法》重要条款

第一章 总则

- **第一条** 为了保障网络安全，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，制定本法。
- **第二条** 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。
- 第三条 国家坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络基础设施建设和互联互通，鼓励网络技术创新和应用，支持培养网络安全人才，建立健全网络安全保障体系，提高网络安全保护能力。
- 第四条 **国家制定并不断完善**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

第一条 --- 第三条，关于维护网络主权和战略规划，明确了网络安全法的目的和适用范围以及国家所应承担的责任义务，方针和原则。
第一条“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申和表现。本条明确了网络安全法制定的目的。网络安全法涉及的范围更为广泛，兼顾了国家安全、社会利益、企业利益和个人权力。
第四条：解决顶层设计问题，同时，说明将来会有配套的法律和制度。

《网络安全法》重要条款

第一章 总则

- 第七条 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，建立多边、民主、透明的网络治理体系。
- **第八条** 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照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。

  县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。
- **第十条** 建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性

第七条，表明国际合作态度
第八条，给出了国家相关监管部门的分工，本法与其他法律的关系。《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，使网络安全监管体制法制化。
第十条，强调了网络数据为保护重点。

《网络安全法》重要条款

第一章 总则

➢ **第十二条** 国家保护公民、法人和其他组织依法使用网络的权利，促进网络接入普及，提升网络服务水平，为社会提供安全、便利的网络服务，保障网络信息依法有序自由流动。任何个人和组织使用网络应当遵守宪法法律，遵守公共秩序，尊重社会公德，不得危害网络安全，不得**利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益**等活动。

➢ **第十三条** 国家支持研究开发有利于未成年人健康成长的网络产品和服务，**依法惩治利用网络从事危害未成年人身心健康的活动**，为未成年人提供安全、健康的网络环境。

第十二条，明确了国家在保障网络安全中的任务和目标，同时对个人及组织使用网络也提出了要求。
第十三条， 加强未成年人保护

《网络安全法》重要条款

第二章　网络安全支持与促进

第二章（共 6 条），要求政府、企业和相关部门通过多种形式对企业和公众**开展网络安全宣传教育，提高安全意识**。鼓励企业、高校等单位加强对网络安全人才的培训和教育，**解决目前网络安全人才严重不足问题**。另外鼓励和支持通过创新技术来**提升安全管理**，保护企业和个人的重要数据。

《网络安全法》重要条款

第二章 网络安全支持与促进	
➢第十九条 各级人民政府及其有关部门应当组织开展经常性的网络安全宣传教育，并指导、督促有关单位做好网络安全宣传教育工作。 大众传播媒介应当有针对性地面向社会进行网络安全宣传教育。	➢第二十条 国家支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流。

第十九条，要求政府或相关部门通过多种形式对企业和公众开展网络安全宣传教育，提高安全意识。
第二十条，鼓励企业、高校等单位加强对网络安全人才的培训和教育，解决目前网络安全人才严重不足问题。

《网络安全法》重要条款

* 第三章　网络运行安全
第三章（共 19 条），特别强调要保障关键信息基础设施的运行安全。安全是重中之重，与国家安全和社会公共利益息息相关。《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。

《网络安全法》重要条款

第三章 网络运行安全

第一节 一般规定

➢**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：

（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

（四）采取数据分类、重要数据备份和加密等措施；

（五）法律、行政法规规定的其他义务。

第二十一条，明确了企业网络安全保护的义务和具体内容。将现行的网络安全等级保护制度上升为法律。

《网络安全法》重要条款

第三章 网络运行安全

第一节 一般规定

➢**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、

➢**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。

第二十二条，主要是对我国网络产品厂商和服务提供商及他们所提供的产品和服务提出了具体的强制要求，不得设置恶意程序，及时向用户安全缺陷、漏洞等风险；

第二十三条，主要是对网络关键设备和网络安全专用产品提出了强制性要求，相关企业在采购过程中要严格审核。

《网络安全法》重要条款

第三章 网络运行安全

第一节 一般规定

➢**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。

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。

第二十四条，提出了上网用户必须实名制。
第二十五条，要求企业必须制定安全应急预案。
第二十六条，第三方服务要守法

《网络安全法》重要条款

第三章 网络运行安全

第一节 一般规定

➢**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；**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**。

➢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。

➢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。

第二十七条，禁止网络犯罪和支持协助犯罪。

《网络安全法》重要条款

第三章 网络运行安全

第二节 关键信息基础设施的运行安全

➢**第三十一条** 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和领域，以及其他一旦遭到破坏、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**关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。**关键信息基础设施的具体范围和安全保护办法由国务院制定。

国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。

➢第三十三条 建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。

第三十一条，定义了关键信息基础设施范围，以及再等保基数上，实行重点保护要求。
第三十三条，强调了企业在建设关键基础设施的三同步原则。

《网络安全法》重要条款

第三章 网络运行安全

第二节 关键信息基础设施的运行安全

➢ 第三十四条 除本法第二十一条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：

（一）设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查

（二）定期对从业人员进行网络安全教育、技术培训和技能考核；

（三）对重要系统和数据库进行容灾备份；

（四）制定网络安全事件应急预案，并定期进行演练

（五）法律、行政法规规定的其他义务。

第三十五条 关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。

第三十六条 关键信息基础设施的运营者采购网络产品和服务，应当按照规定与提供者签订安全保密协议，明确安全和保

第三十四条，对关键基础设施企业的具体安全保护内容提出了具体要求。
第三十五条，建立了关键信息基础设施运营者采购网络产品、服务的安全审查制度。

《网络安全法》重要条款

第三章 网络运行安全

第二节 关键信息基础设施的运行安全

➢**第三十七条** 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，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

➢第三十八条 关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。

➢第三十九条 国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施：

（一）对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估；

（二）定期组织关键信息基础设施的运营者进行网络安全应急演练，提高应对网络安全事件的水平和协同配合能力；

（三）促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享；

（四）对网络安全事件的应急处置与网络功能的恢复等，提供技术支持和协助。

第三十七条，对关键信息基础设施的数据存储办法给了明确定义
第三十八条，要求关键基础设施行业和业主每年必须做检测评估，并明确要求了评估方式和次数。涉及等级测评、风险评估、渗透测试。

《网络安全法》重要条款

* 第四章 网络信息安全
第四章（共 11 条），从三个方面要求加强网络数据信息和个人信息的安全：第一是要求网络运营者对个人信息采集和提取方面采取技术措施和管理办法，加强对公民个人信息的保护，防止公民个人信息数据被非法获取、泄露或者非法使用；第二、赋予监管部门、网络运营者、个人或组织的职责和权限并规范网络合规行为，彼此互相监督管理；第三在有害或不当信息发布和和传输过程中分别对监管者、网络运营商、个人和组织提出了具体处理办法。

《网络安全法》重要条款

第四章 网络信息安全

- **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。网络运营者**不得收集与其提供的服务无关的个人信息**，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。
- **第四十二条** 网络运营者不得泄露、篡改、毁损其收集的个人信息；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。

网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，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。

- 第四十三条 个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。

以上四条都是强调对个人信息的保护。要求网络运营者对个人信息要进行保护，任何人不得非法获取个人信息。

《网络安全法》重要条款

第四章 网络信息安全

- **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。
- **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。

电子信息发送服务提供者和应用软件下载服务提供者，应当履行安全管理义务，知道其用户有前款规定行为的，应当停止提供服 务，采取消除等处置措施，保存有关记录，并向有关主管部门报告。

- 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和举报。

网络运营者对网信部门和有关部门依法实施的监督检查，应当予以配合。

- 第五十条 国家网信部门和有关部门依法履行网络信息安全监督管理职责，发现法律、行政法规禁止发布或者传输的信息的，应当要求网络运营者停止传输，采取消除等处置措施，保存有关记录；对来源于中华人民共和国境外的上述信息，应当通知有关机构采

保障信息安全，进一步完善相关管理制度。

《网络安全法》重要条款

*** 第五章 监测预警与应急处置**

第五章（共 8 条），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。**

《网络安全法》重要条款

第五章 监测预警与应急处置

➢第五十一条 国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。

➢第五十二条 负责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。

➢第五十三条 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。

负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案，并定期组织演练。

网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应

第五十一条、第五十二条：要求国务院有关部门建立监测预警和信息通报机制，加强信息收集、分析及通报工作
第五十三条，行业、业主及部门需按要求建立健全风险评估和应急工作机制，同时按照《信息安全事件分级制度》制定相应的应急预案及应急处置措施，并组织演练、修正与持续改进工作。

《网络安全法》重要条款

第五章 监测预警与应急处置

➢第五十四条 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，采取下列措施：

（一）要求有关部门、机构和人员及时收集、报告有关信息，加强对网络安全风险的监测；

（二）组织有关部门、机构和专业人员，对网络安全风险信息进行分析评估，预测事件发生的可能性、影响范围和危害程度；

（三）向社会发布网络安全风险预警，发布避免、减轻危害的措施。

➢第五十五条 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。

➢第五十六条 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**。网络运营者应当按照要求采取措施，进行整改，消除隐患。

➢第五十七条 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。

➢第五十八条 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。

《网络安全法》重要条款

第六章 法律责任

第六章（共 17 条）

- **行政处罚**：责令改正、警告、罚款，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。

《网络安全法》重要条款

第六章 法律责任

➢第五十九条 网络运营者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的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款；对直接负责的主管人员处五千元以上五万元以下罚款。

关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

第五十九条，网络运营者和关键信息基础设施运营者拒不整改而造成的安全事件或事故，将对整个组织和事件直接责任人将处以罚款。加大了对关键信息基础设施的运营者处罚力度。

《网络安全法》重要条款

第六章 法律责任

➢第六十四条 网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得**一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款**，对直接负责的**主管人员和其他直接责任人员处一万元以上十万元以下罚款**；情节严重的，并可以责令暂停相关业务、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。

违反本法第四十四条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。

第六十四条，对侵害公民个人信息的进行处罚。

《网络安全法》重要条款

第六章 法律责任
➢第六十六条 关键信息基础设施的运营者违反本法第三十七条规定，在境外存储网络数据，或者向境外提供网络数据的，由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、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和其他直接责任人员处一万元以上十万元以下罚款。

第六十六条，关键信息基础设施运营者需要按照法律要求将数据境内存储，若业务需要需向境外传输的需国家网信部门会同国务院有关部门进行安全评估。处罚数据境外存储，向境外提供

《网络安全法》重要条款

第六章 法律责任

➢第六十七条 违反本法第四十六条规定，设立用于实施违法犯罪活动的网站、通讯群组，或者利用网络发布与实施违法犯罪活动有关的信息，尚不构成犯罪的，由公安机关处五日以下拘留，可以并处一万元以上十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处五万元以上五十万元以下罚款。单位有前款规定行为的，由公安机关处十万元以上五十万元以下罚款，并对其直接负责的主管人员和其他直接负责人员依照前款规定处罚。

➢第七十四条 违反本法规定，给他人造成损害的，依法承担民事责任。

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**。

第六十七条，对设立非法网站、通讯群组，发布违法信息进行处罚。
第七十四条，对于违法将承担民事和刑事责任

上海交通大學

SHANGHAI JIAO TONG UNIVERSITY

谢谢！

饮水思源 爱国荣校