网络安全法解读

fanfox7405@163.com

大纲

背景

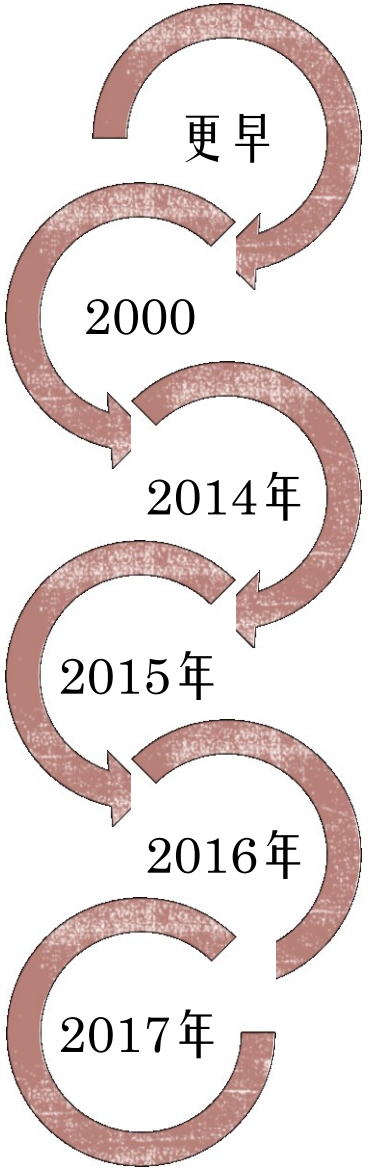
- 应对网络安全威胁已是全球性问题，国际网络安全的法治环境正发生变革，美欧等网络强国纷纷建立全方位、更立体、更具弹性与前瞻性的网络安全立法体系，网络安全立法演变为全球范围内的利益协调与国家主权斗争，有法可依成为谈判与对抗的必要条件。
  - 一是关键信息基础设施安全保障工作亟待加强。电信、能源、交通、金融、政务等关键信息基础设施支撑着相关行业或领域的重要业务，存储着大量个人和业务数据，已经成为网络攻击的重点对象。目前我国关键信息基础设施安全保障整体水平还不高，难以有效抵御有组织大强度的网络攻击。
  - 二是个人和企业权益保护亟待加强。网上非法获取、倒卖个人信息，侵犯知识产权等事件时有发生，严重损害企业和个人的权益，甚至危害个人生命安全。
  - 三是国家安全和社会公共利益面临挑战。恐怖和犯罪组织等，利用网络策划组织暴力、恐怖活动，传播极端、淫秽等信息，甚至意图颠覆国家政权、推翻社会主义制度，严重破坏了社会的和谐稳定，危害公共利益和国家安全。

历史

- **全国人大常委会**–关于维护互联网安全的决定（2000）
- **中共中央办公厅**–《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号）
- **全国人大常委会**–《刑法》2010年修正案

- 6月-十二届全国人大常委会审议了《网络安全法（草案）》
- 7月-向社会公开征求意见，并根据全国人大常委会组成人员和各方面的反馈意见，对草案作了修改，形成了《网络安全法（草案二次审议稿）》

《网络安全法》将于2017年6月1日正式生效。



早期更注重于系统、基础设施等层面的安全立法：

- 国务院-《计算机信息系统安全保护条例》、《互联网信息服务管理办法》
- 公安部-《计算机病毒防治管理办法》
- 公安部等六部委-《信息安全等级保护管理办法》
- 全国人大常委会-《保守国家秘密法》

2014年2月，中央网络安全和信息化领导小组成立，中共中央总书记、国家主席习近平任组长。两会上，“维护网络安全”首次被写入政府工作报告。

- 6月-十二届全国人大常委会对《网络安全法（草案）》进行了二次审议。
- 7月-《网络安全法（草案）》二次审议稿正式在中国人大网公布，并向社会公开征求意见。
- 11月-十二届全国人大常委会第二十四次会议于11月7日上午，以154票赞成、1票弃权表决通过《中华人民共和国网络安全法》。

《网络安全法》概述

- **立法定位：网络安全管理的基础性“保障法”**
  - 第一，该法是网络安全管理的法律。《网络安全法》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》等法律法规共同组成我国网络安全管理的法律体系。因此，需做好网络安全法与不同法律之间的衔接，在网络安全管理之外的领域也应尽量减少立法交叉与重复。
  - 第二，该法是基础性法律。基础性法律的功能更多注重的不是解决问题，而是为问题的解决提供具体指导思路，问题的解决要依靠相配套的法律法规，这样的定位决定了不可避免会出现法律表述上的原则性，相关主体只能判断出网络安全管理对相关问题的解决思路，具体的解决办法有待进一步观察。
  - 第三，该法是安全保障法。面对网络空间安全的综合复杂性，特别是国家关键信息基础设施面临日益严重的传统安全与非传统安全的“极端”威胁，网络空间安全风险“不可逆”的特征进一步凸显。在开放、交互和跨界的网络环境中，实时性能力和态势感知能力成为新的网络安全核心内容。

《网络安全法》概述

- **立法架构："防御、控制与惩治"三位一体**
  - 为实现基础性法律的"保障"功能，网络安全法需确立"防御、控制与惩治"三位一体的立法架构，以"防御和控制"性的法律规范替代传统单纯"惩治"性的刑事法律规范，从多方主体参与综合治理的层面，明确各方主体在预警与监测、网络安全事件的应急与响应、控制与恢复等环节中的过程控制要求，防御、控制、合理分配安全风险，惩治网络空间违法犯罪和恐怖活动。
  - 法律界定了国家、企业、行业组织和个人等主体在网络安全保护方面的责任，设专章规定了国家网络安全监测预警、信息通报和应急制度，明确规定"国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、入侵、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩序"，已开始摆脱传统上将风险预防寄托于事后惩治的立法理念，构建兼具防御、控制与惩治功能的立法架构。

《网络安全法》概述

- **制度设计：网络安全的关键控制节点**
  - 《网络安全法》关注的安全类型是网络运行安全和网络信息安全。
    - 网络运行安全分别从系统安全、产品和服务安全、数据安全以及网络安全监测评估等方面设立制度。
    - 网络信息安全规定了个人信息保护制度和违法有害信息的发现处置制度。
    - 产品和服务强制检测认证制度
    - 关键信息基础设施保护制度
    - 国家安全审查制度
  - 《网络安全法》规定了网络安全等级保护、关键信息基础设施安全保护、网络安全监测预警和信息通报、用户信息保护、网络信息安全投诉举报等制度，以及网络关键设备和网络安全专用产品认证、关键信息基础设施运营者网络产品和服务采购的安全审查、关键信息基础设施运营者信息/数据境内存储、关键信息基础设施运营者信息/数据境外提供安全评估、关键信息基础设施运营者年度风险检测评估、网络可信身份管理、建设运营网络或服务的网络安全保障、网络安全事件应急预案/处置、漏洞等网络安全信息发布、网络信息内容管理、网络安全人员背景审查和从业禁止、网络安全教育和培训、数据留存和协助执法等制度。

《网络安全法》概述

- **重中之重：**关键信息基础设施安全保护办法
  - 关键信息基础设施保护制度是网络安全法若干制度设计的核心之一。
    - 第一，《网络安全法》中明确界定了关键信息基础设施概念的本质，即“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”，并规定关键信息基础设施的具体范围由国务院另行制定。
    - 第二，关键信息基础设施安全保护办法是《网络安全法》中预留接口的下位法，也是法律中唯一明确规定“由国务院制定”的行政法规。我国关键信息基础设施法律制度在法律调整的社会关系及调整对象上更具复杂性。
    - 第三，为了鼓励网络运营者自愿参与国家关键信息基础设施保护体系，促进网络运营者、专业机构和政府有关部门之间的网络安全信息共享，并加强对这些信息的保护，《网络安全法》规定，“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；国家网信部门和有关部门在关键信息基础设施保护中取得的信息，只能用于维护网络安全的需要，不得用于其他用途。”

《网络安全法》概述

明确了网络安全工作的内涵

- 本法广泛征求社会意见，可以说集中了社会各方面智慧，综合了社会各方诉求，最大可能地凝聚社会共识。
- 本法中的网络安全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。

明确了网络安全的工作体制

- 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。

明确了网络安全工作的重点

- 第二章至第五章
- 从网络安全支持与促进、网络运行安全一般规定、关键信息基础设施的运行安全、网络信息安全、监测预警与应急处置五个方面，对网络安全有关事项进行了规定，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。

国家责任和义务

- 定义保护范围
  - 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
- 定义保护原则
  - 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。
- 定义保护战略
  - 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，提出重点领域的网络安全政策、工作任务和措施。
  - 国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩序。
  - 家倡导诚实守信、健康文明的网络行为，推动传播社会主义核心价值观，采取措施提高全社会的网络安全意识和水平，形成全社会共同参与促进网络安全的良好环境。
  - 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。

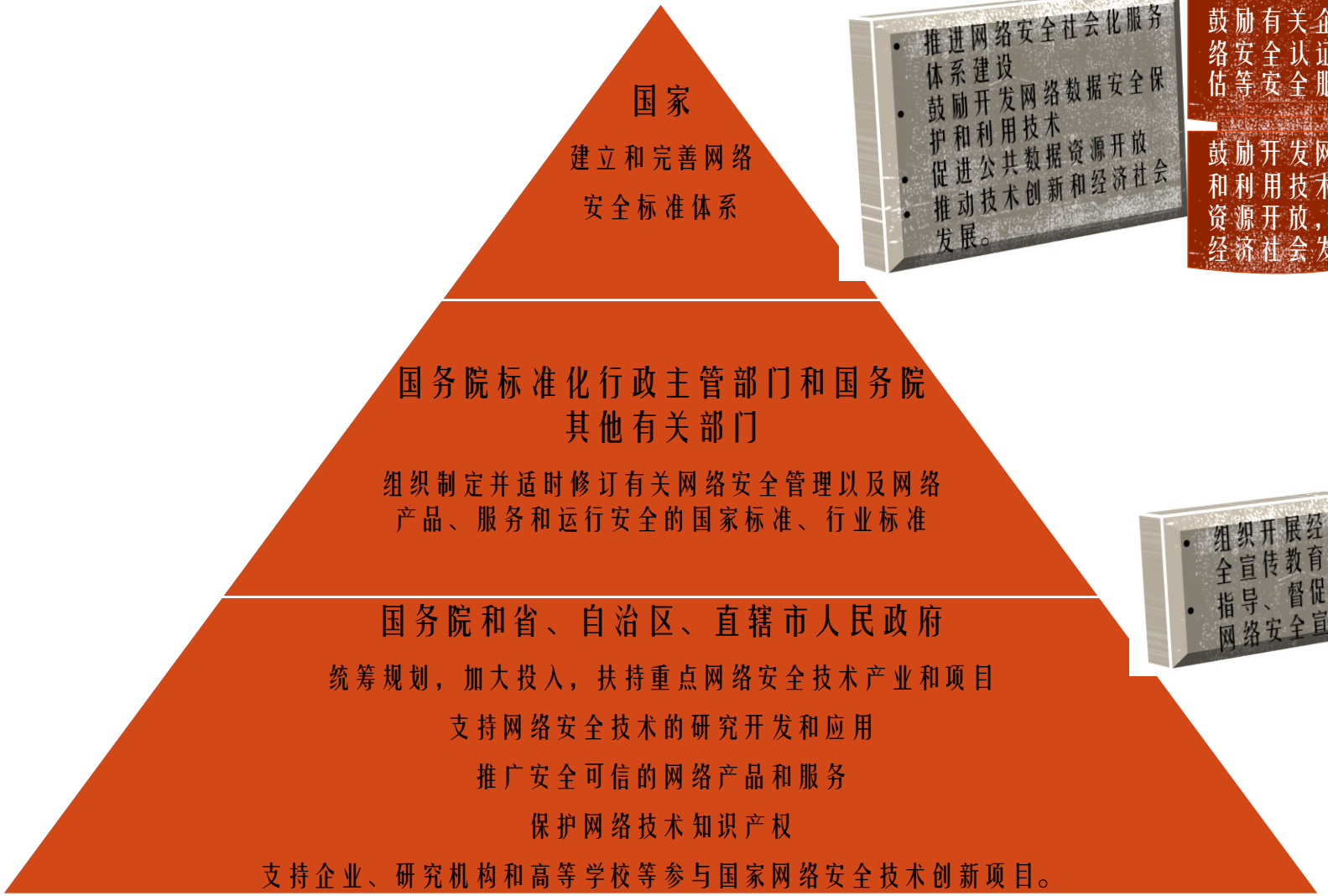
国家责任和义务

- 定义保护职能
  - 行政职能
    - 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。
  - 网络运营机构
    - 开展经营和服务活动，必须遵守法律、行政法规，尊重社会公德，遵守商业道德，诚实信用，履行网络安全保护义务，接受政府和社会的监督，承担社会责任。
    - 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。
  - 相关行业
    - 网络相关行业组织按照章程，加强行业自律，制定网络安全行为规范，指导会员加强网络安全保护，提高网络安全保护水平，促进行业健康发展。

国家责任和义务

- 针对自然人的保护
  - 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。
  - 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。
  - 任何个人和组织有权对危害网络安全的行为向网信、电信、公安等部门举报。收到举报的部门应当及时依法作出处理；不属于本部门职责的，应当及时移送有权处理的部门。
  - 有关部门应当对举报人的相关信息予以保密，保护举报人的合法权益。

网络安全支持与促进



- 推进网络安全社会化服务体系建设
- 鼓励开发网络数据安全保护和利用技术
- 促进公共数据资源开放
- 推动技术创新和经济社会发展。

鼓励有关企业、机构开展网络安全认证、检测和风险评估等安全服务。

鼓励开发网络数据安全保护和利用技术，促进公共数据资源开放，推动技术创新和经济社会发展。

支持创新网络安全管理方式，运用网络新技术，提升网络安全保护水平。

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。

社会责任

- 组织开展经常性的网络安全宣传教育
- 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。

网络运行安全

- 总体纲领
  - 网络安全等级保护制度
- 运营者义务：
  - 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；
  - 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；
  - 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；
  - 采取数据分类、重要数据备份和加密等措施；
  - 法律、行政法规规定的其他义务。

法律责任：
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。

网络运行安全-国家层面

- 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。
- 网信部门会同国务院有关部门（要求）
  - 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。
  - 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。
  - 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。

网络运行安全-网络运营者

- 隐私保护
  - 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。
- 事件处理
  - 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。
  - 遵守国家有关规定，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（各种漏洞发布平台的限制）

    法律责任：
    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。
- 联动
  - 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。

网络运行安全-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。（协会、学会、商会）

网络运行安全-个人、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。

网络运行安全-厂商、服务商

- 符合相关国家标准的强制性要求（如：等级保护）
- 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。
- 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。
- 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。(隐私保护）
- 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。（公安部计算机专用产品销售许可、国家保密局涉密产品测评认证、国家密码管理委员会商用密码产品销售许可、国家信息安全测评中心EAL评级）

关键基础设施保护

- 关键基础设施范围
  - 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
- 保护策略
  - 网络安全等级保护制度的基础上，实行重点保护
- 职责分工
  - 国务院规定的职责分工，负责关键信息基础设施安全保护工作的部门分别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，指导和监督关键信息基础设施运行安全保护工作
- 基础原则要求
  - 安全技术措施同步规划、同步建设、同步使用

法律责任：
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。

关键基础设施保护

- 义务
  - 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；
  - 定期对从业人员进行网络安全教育、技术培训和技能考核；
  - 对重要系统和数据库进行容灾备份；
  - 制定网络安全事件应急预案，并定期进行演练；
  - 法律、行政法规规定的其他义务。
- 保护
  - 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
    - 应当按照规定与提供者签订安全保密协议，明确安全和保密义务与责任。
  - 信息采集
    - 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。
    - 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

法律责任：
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。

关键基础设施保护

- 检查
  - 自查
    - 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。
  - 检查
    - 检查机构
      - 国家网信办-协调
      - 有关部门(-执行
    - 检查要求
      - 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；
      - 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；
      - 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；
      - 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。

法律责任：
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。

监测预警与应急处置


《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》
国家
网络安全监测预警和信息通报制度
职能机构
CERT
CNNVD
公安、国安、保密
工信
……
企业
运营商
高校
安全厂商、机构
IT领域
……
社会团体
安全协会
测评机构
安全团队
……
个人
行业专家
社会型专家
……
国家网信部门
协调
制订应急预案
事件发生
立即启动网络安全事件应急预案
网络安全事件进行调查和评估
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
及时向社会发布与公众有关的警示信息
省级以上相关部门
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

法律责任

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。

- 国家机关政务网络的运营者
  - 由其上级机关或者有关机关责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。
- 网信部门和有关部门
  - 违反本法**第三十条**规定，将在履行网络安全保护职责中获取的信息用于其他用途的，对直接负责的主管人员和其他直接责任人员依法给予处分。
  - 网信部门和有关部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。
- 境外的机构、组织、个人
  - 从事攻击、侵入、干扰、破坏等危害中华人民共和国的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；国务院公安部门和有关部门并可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。
- 与其他相关法的接口
  - 有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。
  - 给他人造成损害的，依法承担民事责任
  - 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。

法律责任-网络运营商

- 未尽管理义务
  - 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。
  - 违反本法第二十六条规定，开展网络安全认证、检测、风险评估等活动，或者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的，由有关主管部门责令改正，给予警告；拒不改正或者情节严重的，处一万元以上十万元以下罚款，并可以由有关主管部门责令暂停相关业务、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五千元以上五万元以下罚款。
  - 对法律、行政法规禁止发布或者传输的信息未停止传输、采取消除等处置措施、保存有关记录的，由有关主管部门责令改正，给予警告，没收违法所得；拒不改正或者情节严重的，处十万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。
  - 电子信息发送服务提供者、应用软件下载服务提供者，不履行本法第四十八条第二款规定的安全管理义务的，依照前款规定处罚。

法律责任-网络运营商

- 未履行协调义务
  - （一）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，采取停止传输、消除等处置措施的；
  - （二）拒绝、阻碍有关部门依法实施的监督检查的；
  - （三）拒不向公安机关、国家安全机关提供技术支持和协助的。
- 由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，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

法律责任-网络运营商

- 恶意损害信息系统
  - 从事危害网络安全的活动，或者提供专门用于从事危害网络安全活动的程序、工具，或者为他人从事危害网络安全的活动提供技术支持、广告推广、支付结算等帮助，尚不构成犯罪的，由公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款。
  - 单位有前款行为的，由公安机关没收违法所得，处十万元以上一百万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。
  - 设立用于实施违法犯罪活动的网站、通讯群组，或者利用网络发布涉及实施违法犯罪活动的信息，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。关闭用于实施违法犯罪活动的网站、通讯群组。
  - 单位有前款行为的，由公安机关处十万元以上五十万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

法律责任-厂商、服务商

- 有以下行为：
  - （一）设置恶意程序的；
  - （二）对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时告知用户并向有关主管部门报告的；
  - （三）擅自终止为其产品、服务提供安全维护的。
- 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，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款

法律责任

- 隐私侵权与保护行为
  - 未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，并可以由有关主管部门责令暂停相关业务、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。
  - 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。

法律责任-关键基础设施

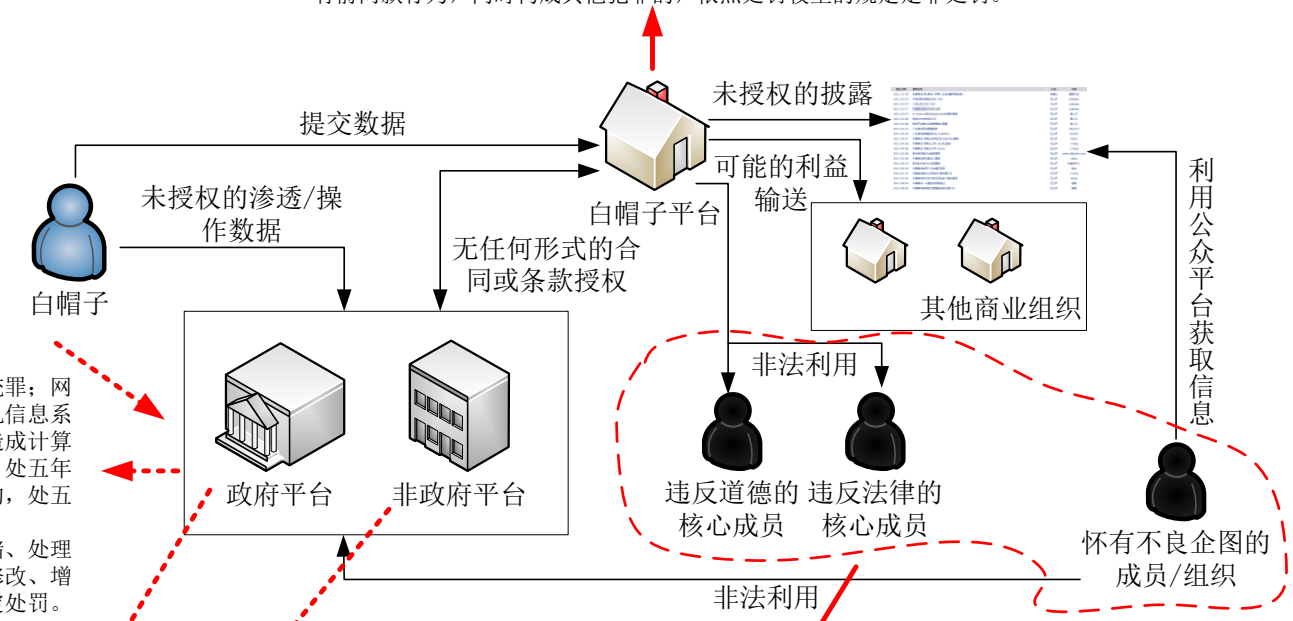
- 未尽保护义务
  - 由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。
- 运营者管理责任
  - 使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令停止使用，处采购金额一倍以上十倍以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。
  - 在境外存储网络数据，或者向境外提供网络数据的，由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；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。

法律责任-人员责任

- 受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。

案例场景

第二百八十七条之二　【帮助信息网络犯罪活动罪】明知他人利用信息网络实施犯罪，为其犯罪提供互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者提供广告推广、支付结算等帮助，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金。
单位犯前款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照第一款的规定处罚。
有前两款行为，同时构成其他犯罪的，依照处罚较重的规定定罪处罚。



第二百八十六条　【破坏计算机信息系统罪；网络服务渎职罪】违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。
违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。

第二百八十五条　【非法侵入计算机信息系统罪；非法获取计算机信息系统数据、非法控制计算机信息系统罪；提供侵入、非法控制计算机信息系统程序、工具罪】违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。

违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

第二百八十七条之一　【非法利用信息网络罪】利用信息网络实施下列行为之一，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金：
(一)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、通讯群组的；
(二)发布有关制作或者销售毒品、枪支、淫秽物品等违禁物品、管制物品或者其他违法犯罪信息的；
(三)为实施诈骗等违法犯罪活动发布信息的。
单位犯前款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照第一款的规定处罚。
有前两款行为，同时构成其他犯罪的，依照处罚较重的规定定罪处罚。

第二百五十三条之一　【侵犯公民个人信息罪】违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

欢迎交流指正

2017年3月27日星期一

解读《网络安全法》

长期合作机构

广东安创信息科技开发有限公司
广州市越秀区寺右新马路 108 号丰伟大厦 15 楼 BC
邮编：510600
电话：+8620-87398319 传真：+8620-87392713