网络主权与网络安全

中国人民大学　许可

FSI2016　2016年12月1日

决策十字阵（Decisional Cross）

理想和价值

过去的经验

未来的愿景

需求和利益

决策十字阵（Decisional Cross）

四种视角

- 国家 VS. 个人

第1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。”

- 安全 VS. 发展

第3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。”

国家的目的与主旨

- 网络安全法的上位法：《国家安全法》

第25条：“国家建设网络与信息安全保障体系，提升网络与信息安全保护能力，加强网络和信息技术的创新研究和开发应用，实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控；加强网络管理，防范、制止和依法惩治网络攻击、网络入侵、网络窃密、散布违法有害信息等网络违法犯罪行为，维护国家网络空间主权、安全和发展利益。”

- 网络安全法的规范基础：网络空间主权

- 网络安全法的“安全”：总体国家安全观

网络空间主权

- 中美两国的核心争议：信息自由VS.国家管制

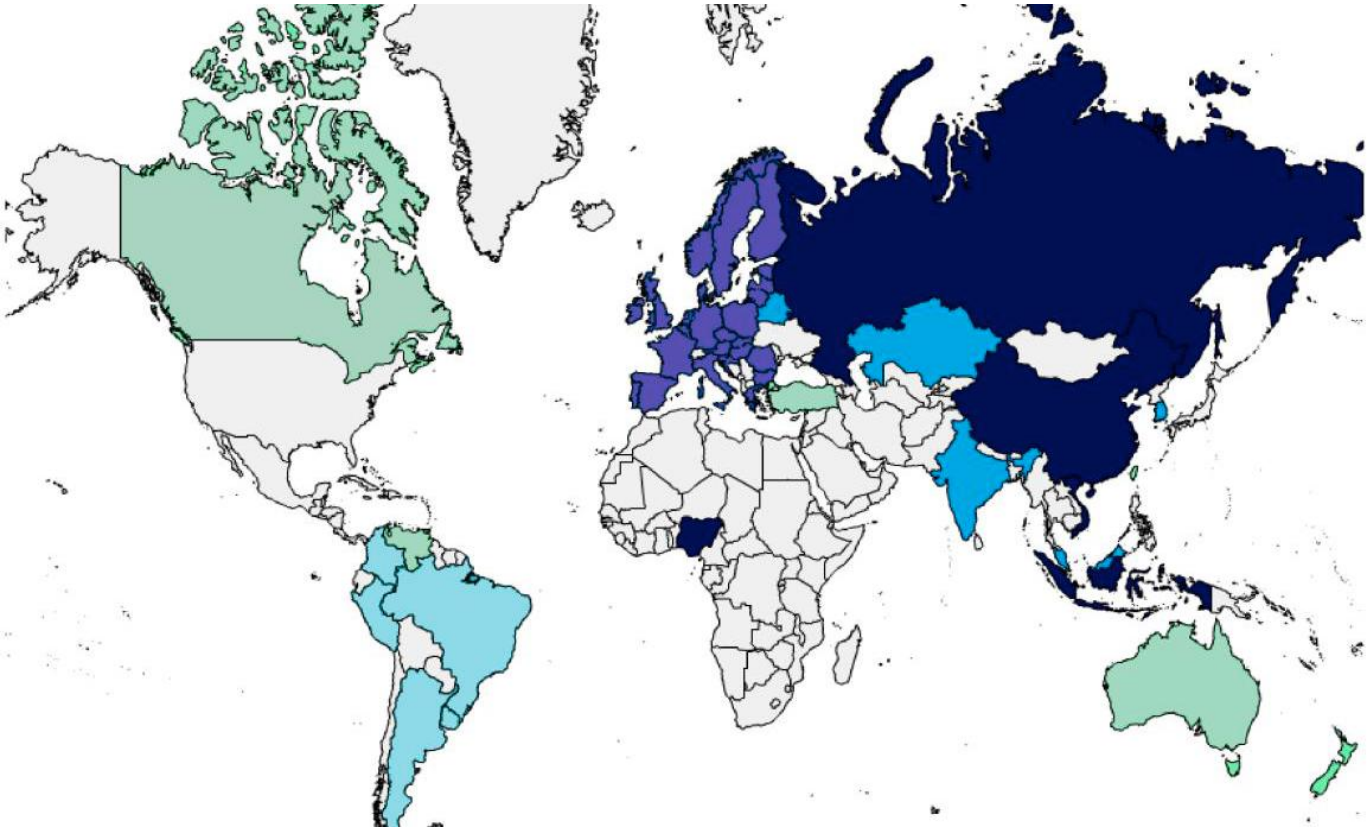
- 信息自由的相对性

法国纳粹物品网络售卖案、欧盟Schrems案

- 数据和服务器的本地化

目前，全球已经有超过60个国家做出本地化存储的要求，
其中既有加拿大、澳大利亚、欧盟等发达国家和地区，
也包括俄罗斯、尼日利亚、印度等发展中国家，

数据和服务器的本地化



网络空间主权的表现

- 网络安全权：即一国所享有的、排除他国对其网络空间恶意侵入和攻击，维护网络信息保密性、完整性和可用性的权利。
- 中国法律的域外效力：
  - 网络设施：旗国原则
  - 网络行为：效果原则
  - 网络主体：国籍原则
- 数据主权：跨境的数据流动控制
- 互联网的国际治理参与权：乌镇世界互联网大会

总体网络安全观

- 国家安全：指国家政权、主权、统一和领土完整、人民福祉、经济社会可持续发展和国家其他重大利益相对处于没有危险和不受内外威胁的状态，以及保障持续安全状态的能力。

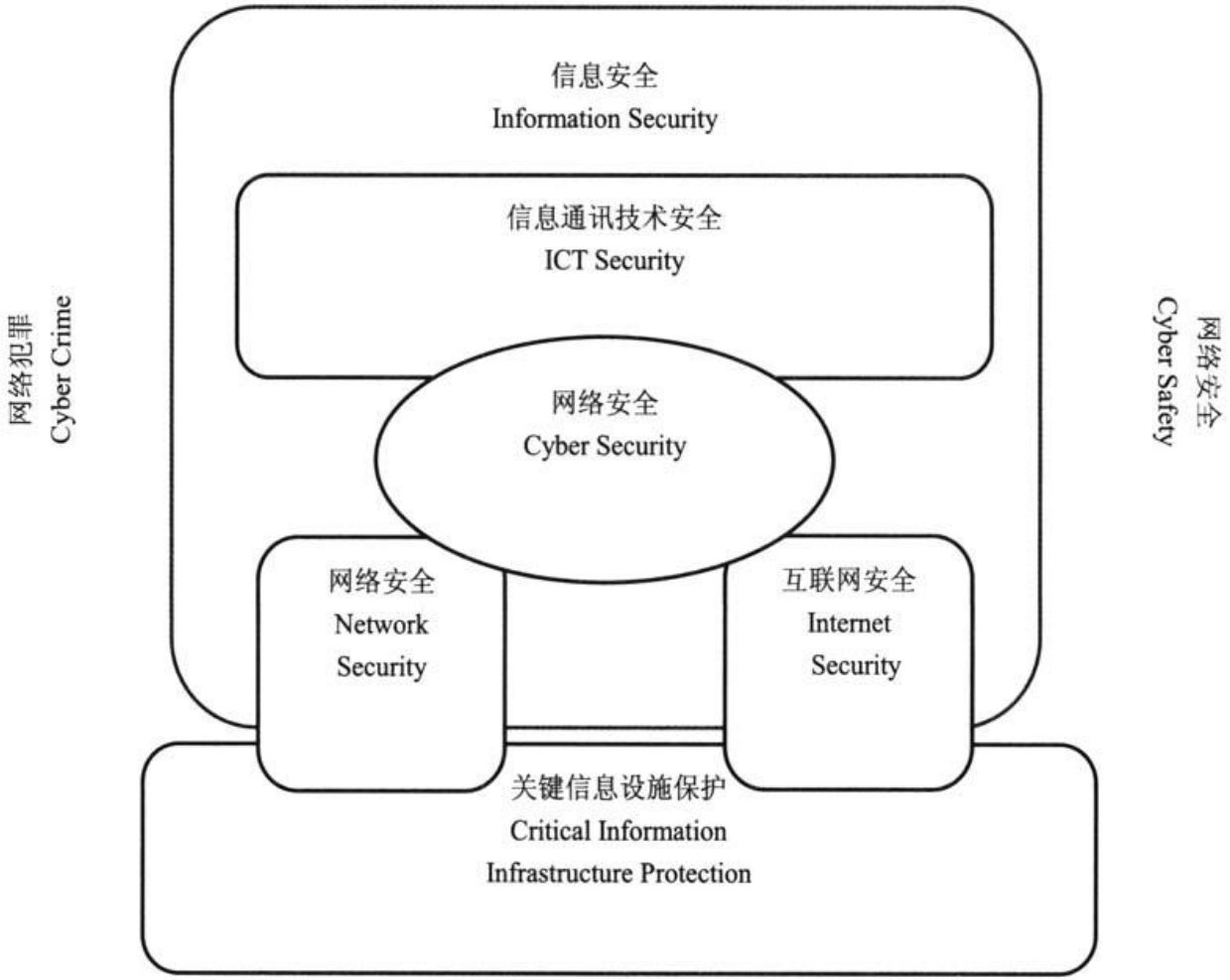
- 网络安全的三层含义

- 信息安全(information security)：网络数据的完整性、保密性、可用性（第76条第2项的后段）

- 网络/因特网安全(network/Internet security)：防范对网络/因特网的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络/因特网处于稳定可靠运行的状态（第76条第2项的前段）

- 网络空间安全（cybersafety）：免受物理的、社会的、精神的、政治的、损害、错误、事故或其他在网络空间不希望发生的事件。（总体国家安全观）

何为网络安全


信息安全
Information Security
信息通讯技术安全
ICT Security
网络安全
Cyber Security
网络安全
Network
Security
互联网安全
Internet
Security
关键信息设施保护
Critical Information
Infrastructure Protection
网络犯罪
Cyber Crime
网络安全
Cyber Safety

个人信息保护

- 个人信息范围：“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”，与2013年工信部颁布的《电信和互联网用户个人信息保护规定》的规定有所限缩，未包含可单独或结合其他信息识别用户使用服务的事件、地点等的信息。

- 收集使用个人信息的“合法正当必要”义务。网络运营者手机和使用个人信息，必须是“合法的、正当的、必要的”，“最小够用”，即不得收集与服务无关的信息，不得违法或违约收集使用个人信息。（第41条）

个人信息保护（II）

- 收集使用个人信息的知情同意义务：网络运营者收集使用个人信息，须公开收集使用规则，明示目的方式和范围，征得被收集人的同意。（第41条第1款）
- 未经同意不得擅自向外提供义务：系“大数据条款”，即“匿名化处理且不能复原的除外”可以向外提供。
- 泄露毁损丢失的及时补救和“双告知”义务：网络运营者具有信息安全保护义务，防止个人信息泄露、毁损和丢失。发生或可能发生的，必须及时补救和双告知（及时告知用户并向有关主管部门报告）。（第42条第2款）
- 删除更正权。赋予个人享有对于网络运营者违法或违约收集使用个人信息的“删除权”和“更正权”。（第43条）
- 不得非法获取、非法出售和非法提供个人信息。（第44条）

安全可控

- 总体要求：安全可信/自主可控/安全可控

- 信息：产品和服务提供者不应利用提供产品和服务的便利条件来非法获取用户系统中的信息、用户设备中自己的信息或者不应该损害用户对自己信息的自主权、支配权，此即用户自己的信息要用户自己作主。

- 系统和设施：产品服务提供者，不能利用提供产品和服务的便利条件来非法控制、非法操纵用户的系统、用户的设备，损害用户对自己系统、设备的控制权，此即系统自己作主。

- 经营活动：网络安全、网络产品和服务的提供者，不应利用用户对产品和服务的依赖进行不正当竞争，谋取不正当利益

网络运营者的安全合规

- 网络安全等级保护义务：网络运营者应当符合网络等级保护制度要求，确定负责人、采取技术措施、留存相关的网络日志等安全保护义务（第21条）。该项义务是对目前已实行的信息系统安全等级保护制度的法定化。例如，1994年国务院颁布《中华人民共和国计算机信息系统安全保护条例》，确立了计算机信息系统安全等级保护制度。1999年公安部颁布《计算机信息系统安全保护等级划分准则》。2007年公安部、国家保密局、国家密码管理局、国务院信息化工作办公室联合发布《信息安全等级保护管理办法》，明确了信息安全等级保护的具体要求。

- 网络实名制义务：网络接入、域名注册服务、电话入网手续、信息发布服务、即时通讯等网络运营者负有网络实名制义务（第24条）。在《全国人大常委会关于加强网络信息保护的决定》的基础上，特别增加了“即时通讯”服务实名制要求。

- 网络事件应急预案、及时补救报告义务。（第25条）

- 网络侦听协助义务：网络运营者为公安、安全机关依法维护国家安全和侦查犯罪提供技术支持和协助（第28条）。

网络运营者的安全合规（II）

- **用户发布信息管理义务和违法信息的停止传输、及时处置及保存记录报告义务**

网络运营者负有网络用户发布信息的管理义务（第47条），与电子信息发送服务提供者和应用软件下载服务提供者一样履行安全管理义务，但对于含有法律法规禁止发布和传输的信息，虽然网络运营者与电子信息发送服务提供者和应用软件下载服务提供者都须立即停止传输，消除处置防扩散，保存记录并报告，但二者的义务又不尽相同，网络运营者是承担主动性义务，即要求主动的“发现”义务，而电子信息发送服务提供者和应用软件下载服务提供者是被动性的“知道”义务。（第48条）

- **网络信息安全投诉举报义务**

建立制度，公布投诉举报方式信息，及时首例并处理投诉举报的义务。（第49条）

网络产品和服务提供者的安全合规

- 不得设定恶意程序
- 网络产品服务安全缺陷漏洞风险的及时补救和“双告知”义务（及时告知用户并向有关主管部门报告）。网络产品和服务安全缺陷漏洞风险的主动发现义务，立即补救，及时“双告知”义务。（第22条第1款）
- 网络产品服务持续安全维护义务。该项义务的立法场景是解决和应对类似微软宣布XP服务更新事件，第22条第2款明确规定了法定和约定期限内的持续安全维护义务。
- 收集用户信息功能的明示同意义务。该项义务多在用户协议情景下，明确提示用户并取得同意。本处的“用户信息”的范围大于用户个人信息范围。（第22条第3款）

网络产品和服务提供者的安全合规（II）

- **网络关键设备和专用产品合格义务。**须遵守强制性标准，并先经合法认证和检测。（第23条）
- 不得非法侵入他人网络、干扰他人网络正常功能、窃取网络数据。（第27条）
- 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。（第27条）
- **不得明知为其提供技术支持、广告推广、支付结算等帮助。**第27条规定本项义务是移植《刑法修正案（九）》第29条明确规定的“帮助信息网络犯罪活动罪”规制的行为类型。

关键信息基础设施运营者的安全合规

- 建设“三同步”义务。主要移植《电信条例》所规定的“同步规划、同步建设、同步使用”义务。（第33条）
- 一般性义务。即在网络安全等级保护义务基础上，还需履行人员安全背景审查、教育培训考核、容灾备份、应急演练等一般性义务。（第34条）
- 网络产品和服务采购的国家安全审查义务。网络产品和服务采购时可能影响国家安全的国家安全审查义务。（第35条）
- 网络产品和服务采购的安全保密义务。（第36条）

关键信息基础设施运营者的安全合规（II）

- **个人信息和重要数据境内存储义务**

“数据本地化存储义务”。（第37条）近年来，在征信、地图、金融、医疗卫生、网络出版及网约车等特殊领域，都明确要求相关数据必须在境内存放和留存，如《征信业管理条例》第24条规定“征信数据”、《地图管理条例》第34条规定“地图数据”、中国人民银行《关于银行业金融机构做好个人金融信息保护工作的通知》第6条规定“个人金融信息”、国家卫计委《人口健康信息管理办法（试行）》第10条规定“各级各类医疗卫生计生服务机构涉及的人口健康信息，不得将人口健康信息在境外的服务器中存储，不得托管、租赁在境外的服务器。不得在境外的服务器中存储”、国家新闻出版广电总局和工信部联合发布的《网络出版服务管理规定》第8条规定“网络出版服务的相关服务器和存储设备”、交通部等七部委联合发布的《网络预约出租汽车经营服务管理暂行办法》27条规定“网约车业务相关数据和信息”等。

- **个人信息和重要数据境外提供的安全评估义务。**一般情况下不允许个人信息和重要数据跨境提供，确需境外提供的，需要依法进行安全评估。（第37条）

- **年度风险检测评估及报告义务。**自行或委托合格机构进行安全风险的检测评估。（第38条）

发展与创新

- 发展的关键在于颠覆性创新：熊皮特的发展理论
- 网络空间是颠覆性创新的优质土壤：作为信用中介的互联网
- 网络空间创新的支持性条件：
  - 政策性促进
  - 互联互通互动的互联网架构
  - 网络空间的竞争秩序

网络安全市场大有可为

- 《网络安全法》多处都明确鼓励有关企业、机构开展网络安全认证、检测和风险评估等网络安全社会化服务，强制要求网络运营者等主体进行网络安全认证、检测和风险评估，必将促进网络安全社会化服务市场大发展。

例如，第17条明确规定国家推进网络安全社会化服务体系建设，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。第23条要求网络关键设备和网络安全专用产品在销售或者提供之前，应当按照相关国家标准的强制性要求经由具备资格的机构安全认证合格或者安全检测。第38条规定，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，开展每年至少进行一次的安全检测评估。第39条规定，国家网信部门在必要时可委托网络安全服务机构对网络存在的安全风险进行检查评估。因此，为了满足网络安全认证、监测和风险评估的合规要求，对于网络安全社会化服务需求会大增，网络安全社会化服务市场大有可为。

多谢聆听，敬请指正！

许可

Email:
xuke_lawyer@163.com

TEL:15801296249(微信)