网络安全法律体系简介

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

主要内容

一、网安法背景

二、网安相关法律体系

三、网安法地位及要点

四、网安法局限讨论

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。**

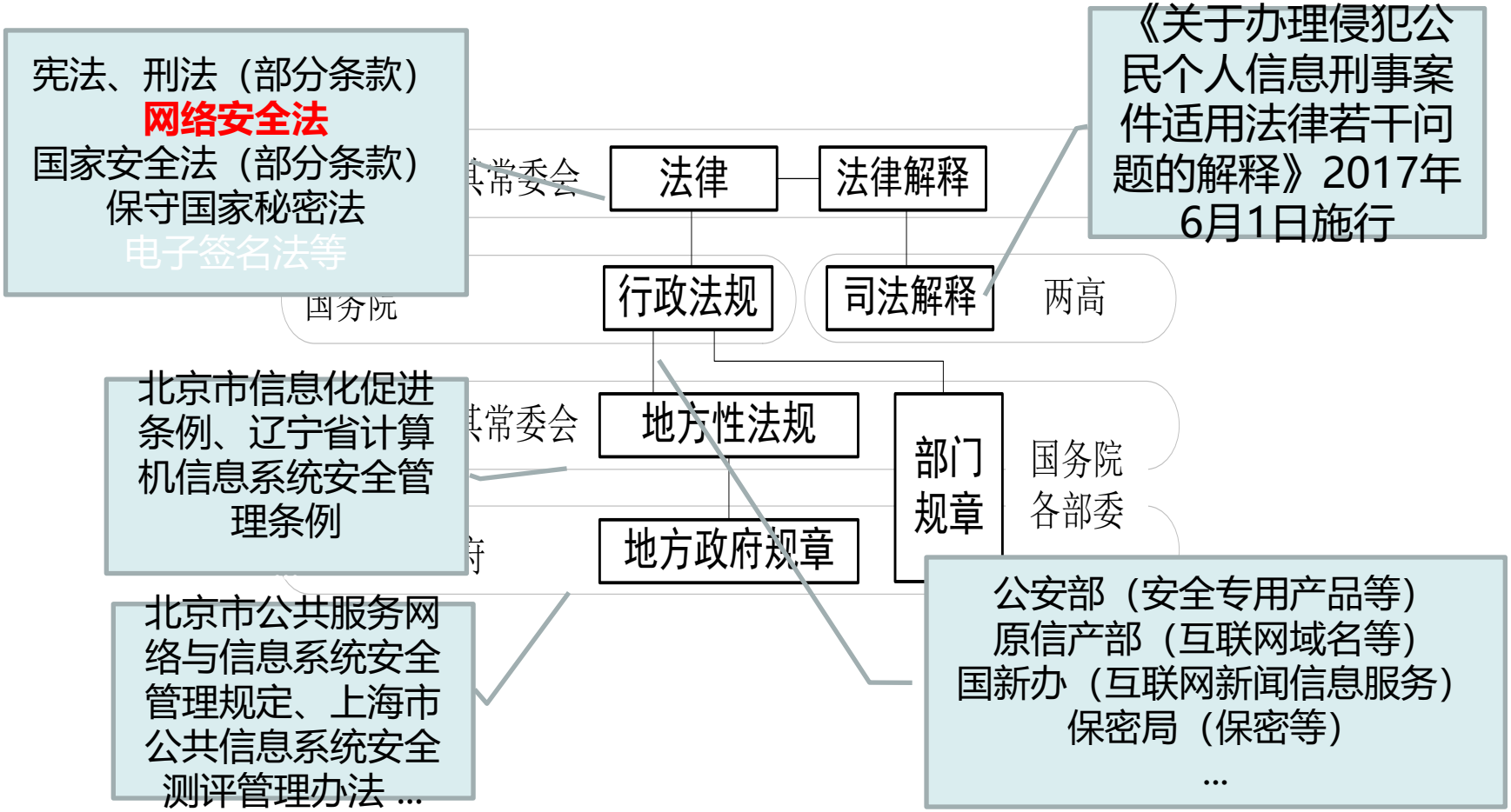
  我国在互联网领域的竞争力和话语权逐渐增强，为了更好地参与互联网国际竞争和国际规则的定制，必须制定和完善国内制度规则，积累中国制度经验。

产生过程

- 更早的讨论可以追朔到2006年之前，当初的定位仅仅是“信息安全条例”、立项讨论《保密法》与“信息安全条例”的关系。
- 2017年6月1日 《网安法》及首批配套法律实施

网安相关法律体系

- 在多级立法的体制下，我国已经先后颁布了一些包含信息安全相关内容的法律、法规、规章等。



与网安法相关的法律法规解读

- 综合性法律：**《网络安全法》**
- 保护国家秘密相关法律
  - 《保守国家秘密法》、《密码法》、《信息公开条例》、《刑法》、《全国人民代表大会常务委员会关于维护互联网安全的决定》等
- 保护商业秘密相关法律
  - 《电子签名法》、《电子商务法》、《反不正当竞争法》等
- 保护个人信息相关法律
  - 《宪法》、《民法典》、《个人信息保护法》、《居民身份证法》、《护照法》、《全国人民代表大会常务委员会关于加强网络信息保护的决定》等
- 保护数据安全相关法律
  - 《数据安全法》、《网络数据安全管理条例》、《工业和信息化领域数据安全管理办法》

地方法规

- 《北京市信息化促进条例》
  - 2007年9月14日公布，自2007年12月1日起施行
  - 适用于北京市信息化工程建设、信息资源开发利用、信息技术推广应用、信息安全保障以及相关管理活动
- 《上海市公共信息系统安全测评管理办法》
  - 2006年5月7日公布，2006年7月1日起施行
  - 适用于上海市行政区域内的公共信息系统安全测评管理活动，具体规定涉及测评的管理部门、责任制度、测评年度计划、新建系统的测评、测评机构、测评协议、测评要求、安全事项告知与协助义务、测评报告、安全整改，对测评机构违法行为的处理等方面
- 《辽宁省计算机信息系统安全管理条例》
- 《重庆市计算机信息系统安全保护条例》
- …

地方规章

- 《北京市微博客发展管理若干规定》（2011年12月16日公布并施行）
- 《北京市公共服务网络与信息系统安全管理规定》
- 《北京市党政机关计算机网络与信息安全管理办法》
- 《上海市公共信息系统安全测评管理办法》
- 《天津市公共计算机信息网络安全保护规定》
- 《黑龙江省计算机信息系统安全管理规定》
- 《辽宁省计算机信息保密管理规定》
- 《大连市人民政府公共信息网络管理暂行规定》
- 《四川省计算机信息系统安全保护管理办法》
- 《山西省计算机安全管理规定》
- 《山东省计算机信息系统安全管理办法》
- 《安徽省计算机信息系统安全保护办法》
- 《河南省计算机信息系统安全保护暂行办法》

- 《广东省计算机信息系统安全保护管理规定》
- 《广东省电子政务信息安全管理暂行办法》
- 《广东省互联网上网服务营业场所管理办法》
- 《广东省计算机信息系统安全保护管理规定实施细则（试行）》
- 《广东省通信短信息服务管理办法（试行）》
- 《深圳经济特区计算机信息系统公共安全管理规定》
- 《福建省互联网上网服务营业场所管理规定》
- 《江苏省互联网网络与信息安全管理暂行规定》
- 《云南省网络与信息系统安全监察管理规定》
- 《江西省计算机信息系统安全保护办法》
- 《杭州市计算机信息系统安全保护管理办法》
- ...

行业规定

- 中国银监会
  - 《电子银行业务管理办法》
  - 《电子银行安全评估指引》
  - 《银行业金融机构信息系统风险管理指引》
- 中国证监会
  - 《网上证券委托暂行管理办法》
  - 《证券期货业信息安全保障管理暂行办法》
  - 《证券公司集中交易安全管理技术指引》
  - 《期货公司信息公示管理规定》（自2009年11月16日起施行）
  - 《深圳证券交易所交易异常情况处理实施细则（试行）》
  - 《上海证券交易所交易异常情况处理实施细则（试行）》
- …

网安法地位与要点

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

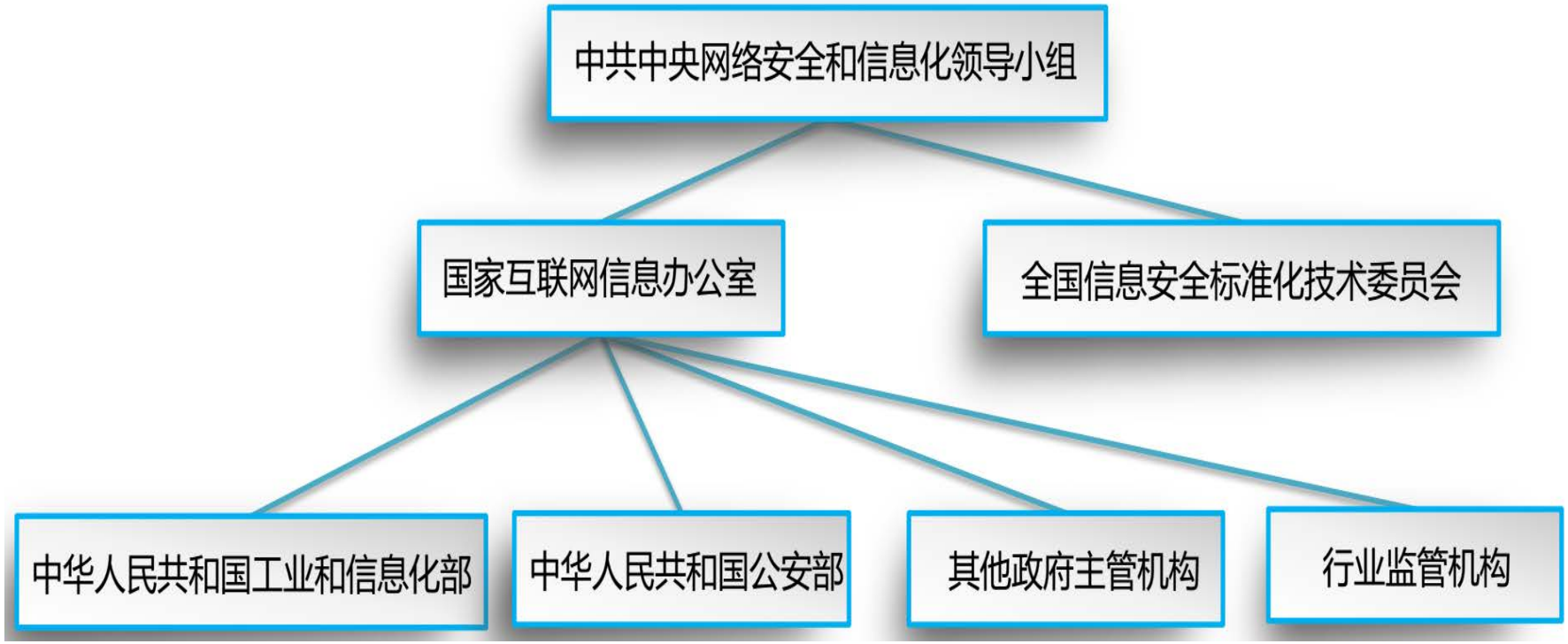
《网络安全法》第4条明确提出了我国网络安全战略的主要内容，即：明确保障网络安全的基本要求和主要目标，提出重点领域的网络安全政策、工作任务和措施。第7条明确规定，我国致力于“推动构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的网络治理体系。”这是我国第一次通过国家法律的形式向世界宣示网络空间治理目标，明确表达了我国的网络空间治理诉求。上述规定提高了我国网络治理公共政策的透明度，与我国的网络大国地位相称，有利于提升我国对网络空间的国际话语权和规则制定权，促成网络空间国际规则的出台。

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。

国家网络安全责任机构组织



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。

明确网络运营者的安全义务

- **内部安全管理**：制定内部安全管理制度和操作规程，确定网络安全负责人
- **安全技术措施**：采取防范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，留存相关的网络日志不少于六个月
- **数据安全管理**：采取数据分类、重要数据备份和加密等措施，防止网络数据泄露或者被窃取、篡改
- **网络身份管理**：办理网络接入、域名注册服务，或固定电话、移动电话等入网手续，或为用户提供信息发布、即时通讯等服务，应要求用户提供真实身份信息。
- **应急预案机制**：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，并向有关主管部门报告。
- **安全协助义务**：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

明确网络产品、服务提供者的安全义务

- **强制标准义务**：网络产品、服务应当符合相关国家标准的强制性要求，不得设置恶意程序；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
- **告知补救义务**：网络产品、服务提供者发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，及时告知用户，向有关主管部门报告。
- **安全维护义务**：网络产品、服务提供者应为产品、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；
- **个人信息保护**：网络产品、服务具有收集用户信息功能的，网络产品、服务提供者应向用户明示并取得同意；涉及用户个人信息的，还应遵守相关法律、行政法规中有关个人信息保护的规定。

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。

网安法局限讨论

- 没有网络安全就没有国家安全
- 总体国家安全观
- 2013年11月，成立中央国家安全委员会

  2014年2月，成立中央网络安全与信息化领导小组

  2015年7月，颁布《国家安全法》

  2016年11月，颁布《网络安全法》

  2016年12月，颁布《国家网络空间安全战略》

国安法

- 国家安全工作应当坚持总体国家安全观，以人民安全为宗旨，以政治安全为根本，以经济安全为基础，以军事、文化、社会安全为保障，以促进国际安全为依托，维护各领域国家安全，构建国家安全体系，走中国特色国家安全道路。
- 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。

国家网络空间安全战略

- 网络渗透危害政治安全。
- 网络攻击威胁经济安全。
- 网络有害信息侵蚀文化安全。
- 网络恐怖和违法犯罪破坏社会安全。
- 以总体国家安全观为指导，贯彻落实创新、协调、绿色、开放、共享的发展理念，增强风险意识和危机意识，统筹国内国际两个大局，统筹发展安全两件大事，积极防御、有效应对，推进网络空间和平、安全、开放、合作、有序，维护国家主权、安全、发展利益，实现建设网络强国的战略目标。

网安法的主体、客体、其他

网络

是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

网络安全

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。

第三章

网络运行安全

网络信息安全

网络安全

第四章

关键信息基础设施

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。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

网络运营者

是指网络的所有者、管理者和网络服务提供者。

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

网络数据

是指通过网络收集、存储、传输、处理和产生的各种电子数据

2011.6，美国军方说网络攻击意味着战争，可和谁开战？

美国还在继续起草应急计划，以防国家遭到大规模网络攻击。一个技术足够先进的敌人能够在战争时期（或发动攻击之前）切断军事通信，但更有可能成为目标的是美国的民用基础设施，包括公用事业和金融市场。

2019.7，网络攻击引入战争思维：“先发制人”，美国就能决胜疆场？

特朗普授权美国网络司令部自主判定来自世界的网络攻击意图，赋予他们在网络世界可以将任何国家先打一顿再说的特权。

2021.7，美国总统拜登当地时间27日表示，美国如果遭到重大网络攻击，可能会与一个“大国”进行“真正的枪战”。

世界应该建立这样的共识：

美国摒弃了网络世界的防御优先战略，而“先发制人”成为美国的网战新规则。

美国的网络战略无论在技术上、法律上还是规则上都具备强烈的主动攻击性！

我们应该建立什么样的网络安全法？

第四次研讨题目

网络安全法79条

4.1

网络安全审查办法23条

4.2

关键信息基础设施保护条例55条

4.3

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

Thank You!

Tel: 86-10-8254**** Fax: 86-10-8254****
E-mail: ***@iie.ac.cn
地址：北京市海淀区闵庄路甲89号 100093