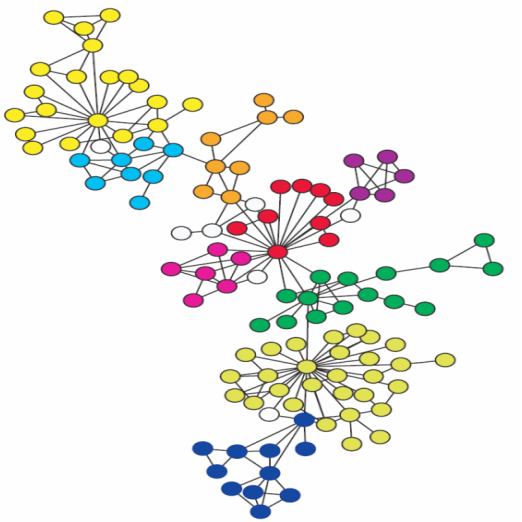
网络安全面临的严峻挑战与若干应对建议

——专家媒体评论综述

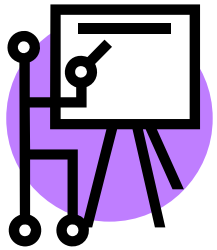


方锦清

中国原子能科学研究院，北京

Email: fjq96@126.com

目　录



一、引 言

21世纪是一个网络信息时代，网络安全问题成为最突出的全球性问题之一，它不仅是一个纯技术性问题，而是与社会、政治、军事等紧密关联的错综复杂的综合安全问题。与各个国家及世界上每个人都息息相关。

网络安全的态势

- 今年，美国炒作“中国黑客威胁论”，甚嚣尘上，旨在制造一场有计划、有目的、有组织的舆论战，以为其今后进行的网络进攻寻找借口。
- 当前我国大多数黑客攻击来自美国。国际上一些发达国家随之紧跟，“网络空间战”已纳入北约和澳大利亚等国战略。日本、法国、德国、印度等国家都已建立成编制的网络战部队。
- 我国面对国际上的严峻挑战，我国决不能等闲视！

中美元首通话交流网络安全

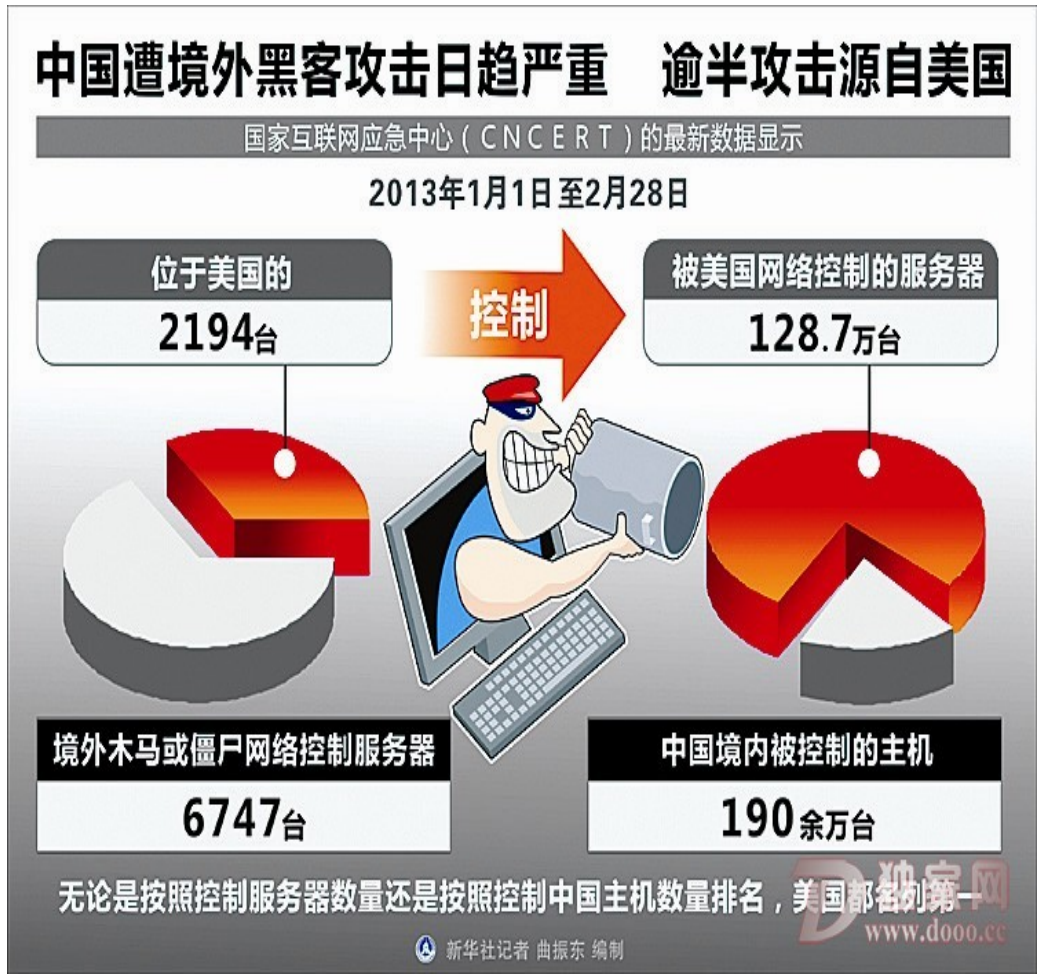
- 国家主席习近平于3月14日应约同美国总统奥巴马通电话时，就网络安全问题交换了意见。
- 习近平主席阐述了中方原则立场，表示当前网络安全问题日益突出，已成为各国普遍关切的综合安全挑战。维护网络空间的和平、安全、开放、合作，符合中美在内的国际社会共同利益。中方坚决反对任何形式的黑客活动。中方愿同美方以建设性方式就网络安全问题保持沟通。

外交部发言人华春莹2013.3.15日在例行记者会上公开了通话内容

- 美国由于军事需要1969年创造了互联网，在网络空间方面，具有绝对的主导地位和优势，美军是第一个谋划网络战的国家，也是第一个进行网络战的国家，他们这方面动作频频。
- 中国是全球网络发展最快的国家之一，同时也是遭受网络攻击最严重的国家之一。
- 网络犯罪和网络恐怖主义的危害也在日益凸显。网络诈骗、网络盗窃以及制作传播计算机病毒、入侵和攻击计算机网络等犯罪活动，直接影响政府施政和社会正常运转。“网络恐怖主义危害也在上升，恐怖组织利用网络空间进行招募、培训、煽动和组织活动，危害各国和地区安全，极端势力利用网络平台宣传非法主张、策动破坏行动，对一些国家安全稳定造成威胁。

我国的黑客威胁主要来自美国

中国国家计算机网络应急技术处理协调中心（CNCERT）的数据显示，与西方个别媒体报道正好相反，中国才是网络攻击的受害者。侵害中国月均遭攻击8万余次，IP地址显示大多源自美国。



美国国防部长帕内塔一语道破天机

- 2012年11月演讲称：网络安全部门需要更多的财政和人力资源，“我们吸纳了很多优秀人才参与（网络安全）。面对正在发生的变化，如果想一直保持前沿地位，我们必须在这个领域投入更多。”
- 制造中国网络威胁论就是为了增加扩大网军的经费
- 网络战已经远超“把XX官方网站黑掉”的层次，而发展为通过互联网摧毁敌国电力、金融、通讯、作战指挥等关键系统的战争力量。
- 今年3月15日，美国网络战司令部司令亚历山大宣布，美军将新增40支网络部队。

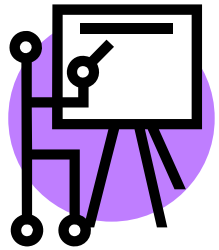
我国外交部长杨洁篪回答了记者关于网络黑客问题

2013年3月7日我国外交部长杨洁篪回答了记者关于网络黑客问题的提问，指出：“近有关黑客攻击的报道很多，不少拿中国说事。看起来挺抓眼球，实际上经不起推敲。事实上，中国在网络安全方面是弱势群体，中国是受黑客攻击最严重的国家之一。中国政府坚决反对黑客攻击行动，已经制定了相关的法律规定，明确禁止和打击黑客攻击活动。”

“我想人们没有患色盲症，黑的就是黑的，白的就是白的。出于政治目的编造和拼凑耸人听闻的新闻，既抹黑不了别人，也洗白不了自己。”

我国政府的严正立场

- “各国在网络空间是一个你中有我、我中有你的“命运共同体”，网络空间需要的不是战争，而是规则与合作。我们反对把网络空间变成另一个战场，把网络作为干涉别国内政的另一个工具。
- 中方一直倡导构建一个和平、安全、开放、合作的网络空间，主张在联合国框架内制定相关的国际规则，并提出了具体的倡议。我们希望有关方停止不负责任的攻击和指责，采取切实行动，增进各方互信与合作，共同维护网络空间的和平与安全。”



目 录

网络空间安全面临空前挑战

网络空间是主权国家在陆、海、空、天之外的“第五空间”，网络空间的出现，使国家安全涵盖的空间从传统的扩大到了“信息边疆”。网络信息传播突破了时空限制，对传统安全防范体系造成了严重冲击。它已经成为是主权国家赖以正常运转的“神经系统”。

网络空间安全面临空前挑战

- 网络空间不应该成为另外一个战场，需要的是规则和合作。
- 网络空间及其资源是全人类的共有财富，维护网络空间安全符合我们包括世界人民的共同利益。各国应以更加开放的博大胸襟、更积极的建设性态度，同舟共济，携手合作，共同制定网络空间的规则，深化打击网络跨国犯罪的合作，加快网络防护技术研发，完善网络安全对话机制，建立和谐的网络世界。

第一，大搞网络心理战，企图影响和破坏我国政治社会稳定

第二，间谍机构密集攻击我国重要部门信息网络

第三，愈来愈猖獗的信息网络违法犯罪活动和侵权行为

- 网络洗钱、网络诈骗、网上黄赌毒等犯罪活动蔓延全世界，智能手机移动网络更使犯罪分子如虎添翼，一个网络地下黑色产业链正在形成。网络社会正在全方位复制并不断翻新现实社会的犯罪形态，目前我国《刑法》已难以涵盖现实中发生的信息网络犯罪类型。
- 同时，“人肉搜索”、“网络暴力”、“网络谣言”、“网络抄袭剽窃”等网络侵权行为愈来愈严重，而网络维权，寻求法律保护和司法救济迫在眉睫。

第四，网络战准备正在紧锣密鼓进行，严重威胁我国的网络安全

- 据美国防务专家乔尔·哈丁2010年的评估，美军网络战部队总数近9万人。随着近年来的不断壮大，目前数量已经超过10万人。一支规模如此庞大的网军，一旦集中发动攻击，任何国家和机构都将难以承受。
- 可见：美国指责中国网络攻击，完全是贼喊捉贼，根本不值一驳。美军黑客部队有10万大军，世界最强，掌握全世界最先进的网络攻防能力。

美国黑客部队总数超10万
扩大网络司令部

- 2002年组建网络黑客部队，建有专门的黑客部队超10万人，并在全球范围内招募黑客精英为其服务。
- 2009年成立网络司令部，司令部人员有937人，准备扩大到4900人.刚成立时经费是1.5亿美元，2013年增加到1.8万亿美元。
- 美国建立名为“梯队”的窃听系统，拥有120多个卫星网站，对全球进行窃听，“梯队”系统作为一个由美国操纵的情报收集分析网络，能够在全球范围内拦截以公众电话交换网络、卫星及微波通讯所传送的电话、传真、电子邮件和其他数字资讯等。

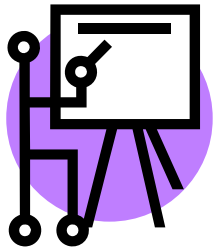
美军网络司令部徽标。美军黑客总部周围雷达及天线密布（中国国防报图片）。

中国网 china.com.cn， 2013-02-28 央视国际

美国网络司令部将组建三类部队

1. “国家任务部队”，负责保护电网、发电厂以及其他对国家安全和经济安全至关重要的基础设施
2. “战斗任务部队”，帮助指挥官制定境外行动计划、发动攻击以及采取其他进攻性行动
3. “网络保护部队”，用于加强保护国防部的网络

目　录



网络战的三大使命

情报战

窃密与反窃密、，间谍案、遥控木马、破解、窃听，勾结

系统战

对信息系统破坏/控制与安全防护/反控制破坏数字武器、数字战场、国家重要基础设施

心理战

网络舆论煽动、渗透、篡改与舆情治理

Web2.0、P2P、WAP、WEB、 Email

网络战中需要重点保护的国家网络

- 国家电子政务重要领域网络：党政、人大、政协

军用-战争网络

- （8+2工程）：

  电力、金融、民航、铁路、海关、证券、保险、税务、广电网、电信网

- 自动化、信息化、网络化支撑的产业供应链，国际化跨部门、行业、地区、国界的信息网络

应对“网络珍珠港”的可能性

- 2012年8月沙特阿拉伯的网络遇袭事件令帕内塔十分担心。
- 2012年10月帕内塔警告称，美国正面临着一个“网络珍珠港”的可能性。因此，尽管目前国防部正在大幅削减开支，包括削减对传统地面武装人员的投入，却仍旧做出了扩充网络安全部队的决定。这反应出美国对网络安全战争日益重视的态度。

三种主要网络攻击形式

境外通过木马或僵尸网络控制境内主机

2012年，根据CNCERT抽样监测发现，境外有73286个IP地址作为木马或僵尸网络控制服务器参与控制我国境内受控主机近1419.7万个。其中位于美国的控制服务器控制了我国境内近1051.2万个主机IP，控制我国境内主机IP数量居首位，其次是位于韩国和德国的IP地址，分别控制了我国境内近78.5万个和近77.8万个主机IP。

利用境外注册域名传播恶意代码

2012年，在CNCERT监测发现的放马站点（指攻击者存放恶意程序的网络地址）中，放马站点所利用的恶意域名月均有65.5%在境外注册，严重威胁着我国互联网用户上网安全。

境外攻击境内网站

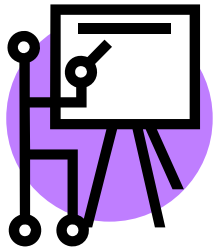
一部分是通过植入后门对境内网站实施远程控制，美国就有7370个IP（占22.9%）控制着我境内10037个网站，位居第一。还有采取直接网页仿冒的手段。2012年，CNCERT监测到仿冒境内网站的服务器IP有96.2%位于境外，其中美国和中国香港居前两位，分别承载了18320个和2804个仿冒页面。

美国研发出两千多种“网空”武器

- 目前，美军已开发出“蠕虫”病毒、逻辑炸弹等2000多种“网空”作战武器。
- **2012年7月11日，美国国防部发布了《云计算战略》，明确未来美军云计算的发展步骤、管理方式和发展思路，标志着美军的军用“云计算”技术大规模建设和推广工作正式启动。**
- 美军网络司令部司令兼美国国家安全局局长基思·亚历山大表示，政府需要在攻击发生之前将其扼杀，采取何种防御措施部分归因于攻击手段。

- 2012年11月20日，美发布了“基础网电作战”项目是国防高级研究计划局（DARPA）发展网络攻击型武器的一个项目，标志着美国网络空间初具雏形的军事行动进入了新阶段。DARPA开始为网络空间攻击能力构建平台，并呼吁学术界和工业界的专家参与。
- 美国认为，控制网络空间对国家安全至关重要。因此，美军网络司令部正在获得一组能力，它们能为军事和政府决策者建立灵活的选择。这些能力可能但不限于以下：威慑对手、拒绝对手进入和作业、中断对手、欺骗对手、劝阻对手、打败对手等能力。网络司令部正通过开发和部署一系列进攻性和防御性、摧毁性和非摧毁性、致命性和非致命性武器来实现上述能力。

目　录



美网络实战化的案例

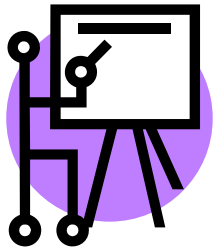
- 美军的网络战武器已经在多场战争针对多个国家使用。在海湾战争、伊拉克和阿富汗战争中，都有报道美军大量计算机病毒武器投入战场使用。近年来，美军更是频繁使用网络战武器

- 据美国媒体报道，2010年12月为瘫痪伊朗布什尔核电站，从而阻挠该国的核开发，美国连同以色列向伊朗的计算机系统植入“震网”病毒，导致离心机运作出现问题。 。“震网”的“蠕虫”病毒是世界上首个得到公开证实的武器级软件，一些人称它为“数字制导导弹”。

- 在2011年3月19日开始的利比亚战争中，美军在战争爆发前夕，干扰和入侵利比亚的互联网和通讯网，给其高级将领的手机发送策反短信，并以卡扎菲父子直接统领的第9旅和第32旅为目标，实施电子渗透和网络攻击。美军甚至还研制了一种病毒，能使对方的显示器屏幕出现难以觉察的闪烁，造成操作人员发生视觉疲劳和莫名的头痛，这可以算作是一种网络生理战武器。

- 2011年，美国继续建设国家网络靶场，依托靶场测试新型网络攻防技术，并对攻击效果进行可靠性评估。2012年5月28日，一种名为“火焰”的计算机病毒作为超级网络武器，攻击了伊朗等国的许多计算机。这是迄今为止最为强大的网络炸弹，威力是2010年网络炸弹“震网”的20倍。

目　录



2012网络安全十大事件及2013重大威胁预测

知名信息安全厂商卡巴斯基实验室

- 对未来一年的预测主要包括继续增长的针对性攻击、网络间谍攻击和国家级网络攻击的加剧、黑客主义的演化、具有争议性的所谓“合法”监控工具的发展以及针对基于云的服务网络犯罪攻击加剧。

1	针对Mac OS X系统的复杂恶意软件出现
2	安卓系统威胁呈爆炸式增长
3	Flame和Gauss的出现表明某些国家仍然在背后支持网络战争行动
4	大规模网络服务密码泄漏事件，例如LinkedIn和Dropbox
5	Adobe数字证书失窃事件
6	Java和其它常见软件出现最新零日漏洞
7	针对网络设备的大规模攻击（即DSL路由器）
8	DNSChanger服务器被关闭
9	破坏性恶意软件Shamoon和Wiper的出现
10	Madi网络间谍攻击行动

2013 预测

1	“黑客主义”继续蔓延
2	将出现更多政府资助的网络攻击
3	政府支持在网络空间使用所谓的“合法”监控工具
4	针对基于云的基础设施攻击加剧
5	数字隐私信息情况恶化
6	在线验证和数字认证机构仍将面临各类问题
7	Mac OS X恶意软件和手机恶意软件数量持续增多
8	网络罪犯仍然利用漏洞和利用程序做为主要攻击手段
9	勒索软件和加密勒索软件泛滥

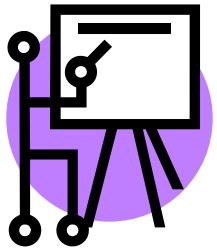
2013年互联网六大威胁

http://www.enet.com.cn/security/

2012年12月26日17：33 来源：中关村在线 作者:王宪阁

1. APT攻击移动平台
2. 双因子安全认证取代但密码认证
3. 攻击物联网
4. 突破沙箱攻击
5. 跨平台的僵尸网络
6. 移动恶意软件数量激增

目　录



保障网络安全的迫切需求

- 信息网络虽然是信息技术发展的产物，但是，保护信息网络安全，不仅需要先进技术，更需要法律、道德等有力支撑。加强信息网络安全管理，呼吁法治建设，依法建网、依法用网、依法管网，是保障网络安全的迫切要求。

维护国家网络主权的迫切需求

•某些西方国家极力渲染和推销“国家主权过时论”，企图实现网络霸权。我国必须依法对网络行使主权管辖权，维护网络空间国家主权，迫切需要加强网络法治建设。

维护网络安全秩序的迫切需求

•信息网络绝不是一方净土，同现实社会一样,既存在着真、善、美，也滋生着假、恶、丑；既是网民和“机民（手机用户）”的数字化乐园，也是恐怖分子和违法犯罪分子的避风港。必须依法规范网络秩序，重组网络空间权利与义务关系，营造良好网络环境，迫切需要加快网络法治建设。

应对网络突发危机的迫切需求

•信息网络具有不经时间验证和过滤的瞬间聚集性，极易促使潜在的紧张关系迅速转化为突然的冲突，产生危机，并可以迅速使局部问题“全局化”、简单问题“复杂化”、普通问题“政治化”、一般问题“热点化”。因此，依法规制网络行为和管理措施，确保应对网络突发危机的信息主动权，必须加强网络法治建设。

防范解决网络纠纷的迫切需求

•我国网络纠纷案件日益增多，而且越来越国际化和政治化，比如，2010 年腾讯和“360”之间的不正当竞争，美国谷歌公司的“搜索引擎”纠纷等，已严重威胁到中国信息安全。因此，要使网络主体行而有据，司法机关裁而有度，有效地防范和解决各种网络纠纷，就必须加强网络法治建设。

加强网络监管治理的迫切需求

•受某些西方国家鼓吹的“网络监管有损言论自由”，“严格监管将削弱和抹杀技术创新”等观点影响，我国在网络监管上思想不统一，认识有分歧。追求自由、平等和共享是网络的理想目标，维护秩序、公正和安全是网络的现实要求，平衡这两者的关系，需要加强网络法治建设，依法实施政府介入的、适度的网络法制监管治理。

走我国独立自主的互联网创新发展之路

- 制网权是与互联网共存亡的一种新型国家权力，是一个主权国家在网络空间生存的根本保障，是国际政治领域中国家权力的新型构成要素。
- 为了维护与实现我国、民族的现实与长远利益，必须大力增强提高本国互联网的控制力和引导力，走独立自主的创新的互联网发展道路。
- 研发具有自主知识产权的硬件技术、软件设备等，这是保障信息安全的重中之重，也是强化国家网络安全的重要措施。

网络安全的关键技术

防火墙技术

1. “防火墙”是一种形象的说法，其实它是一种由计算机硬件和软件的组合，使互联网与内部网之间建立起一个安全网关(scurity gateway)，而保护内部网免受非法用户的侵入。所谓防火墙就是一个把互联网与内部网隔开的屏障。

数据加密技术

为提高信息系统及数据的安全性和保密性，防止秘密数据被外部破析所采用的主要技术手段之一。 1)数据传输加密技术 :常用的有线路加密和端——端加密两种; 2)数据存储加密技术; 3)数据完整性鉴别技术; 4) 密钥管理技术

智能卡技术

3. 智能卡就是密钥的一种媒体，如同信用卡，当口令与身份特征共用时，其保密性能相当好。网络安全和数据保护这些防范措施都有限度，并非越安全就越可靠。因而，在看一个内部网是否安全时不仅要考察其手段，而更重要的是对该网络所采取的各种措施，其中不光是物理防范，还有人员的素质等其他“软”因素，进行综合评估，从而得出是否安全的。

空间网络安全的关键技术研发

- 多层次空间网络的理论体系 由部署在不同轨道、执行不同任务的多种类型的卫星、临近空间飞行器及相应地面系统和终端连接起来,并与传统地面有线和无线网络相融合的空天地一体化网络。
- 空间网络的安全技术研究：针对空间网络具有复杂性、异构性、信道开放性等特点对空间组网安全是巨大的挑战。
- 信息支撑技术：实现快速智能的信息获取、传输、处理、分发和应用,将成为未来信息化战争的技术支撑,对国防现代化建设具有巨大的推动作用。
- 空间网络的基本问题研究（研究热点之一）：如何设计满足空间网络应用要求和特点的安全解决方案。
- 新网武技术：离线攻击技术和无线注入进攻技术

美军无线网络攻击能力进展惊人

- 12年前，美军正在研发的“舒特”项目被媒体曝光，一时令世界各国震惊，有人说它将彻底改变未来战争模样。
- 长期潜于水下的“舒特”项目以美国“红旗”演习发起人理查德·穆迪·舒特上校的名字命名，这种绝密的攻击手段是一种通过无线方式进入对手信息网络、瘫痪对手防空体系的武器系统，作战效益巨大。
- 一系列迹象却表明，美军“舒特”项目不仅存在，而且在技、战术方面已经获得长足进展，正在成为战场网络空间一个威力惊人的“潘多拉”魔盒。
- “舒特”正在小型化，向隐身无人机和作战飞机上改装。这样，美国拥有了能遏制敌空中和海上防御的网络武器。

增强对国际互联网的控制力和引导力

这种控制并非强制和垄断，而是能够及时有效地预测、防范和应对非法行为通过国际互联网对我国家利益的损害。

- 倡导与定位“互联网主权”的国际法理地位
- 力争IPv6资源，加快下一代互联网建设

必须加强和完善网络法治建设

- 我国信息网络法治建设起步于20世纪80年代，经过近30年的发展，初步形成了网络法律法规体系。
- 从总体上看，我国网络法治建设水平还不高，法治防线缺口很大，存在主要问题：

网络法治理念滞后

网络法学研究薄弱

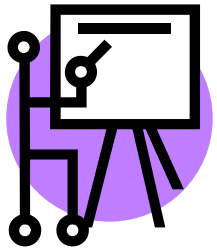
网络立法缺乏总体规划

缺少网络电子治理措施

网络法律资源匮乏

无诚信的法治规制和道德准则

目　录



七、加强网络安全的国际合作 共建和谐绿色的网络世界

- 网络空间已被视为继陆、海、空、天之后的“第五空间”。世界既深得网络发展之利又深受网络攻击之害。网络空间安全问题已成为困扰世界的严峻挑战。对于网络空间安全问题:
- 首先，要尊重各国在网络空间的主权，这是对“尊重主权”这一国际法原则的继承和发展。
- 第二，要和平利用网络空间，制止网络空间军备竞赛。
- 第三，要依法维护网络空间秩序。

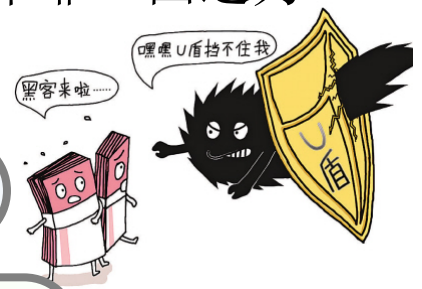
近年来，虽然多个国家纷纷制定网络政策，完善相关法律法规和管理制度，但是网络空间治理水平还需要进一步提高。

制定网络空间的国家行为准则

- 中国是互联网大国，但不是互联网强国，大量事实证明，中国多年来一直是网络攻击的主要受害国之一。
- 中国政府一贯坚决反对并依法打击黑客攻击行为。为推动解决网络安全问题，2011年9月，中国与俄罗斯等国向联合国共同提交了“信息安全国际行为准则”草案。
- 中方呼吁国际社会以此为基础，制定网络空间的负责任国家行为准则，共同构建一个和平、安全、开放、合作的网络空间，维护国际社会共同利益。
- 发挥联合国的主渠道作用，充分听取各方意见，平衡处理各方关切，务实推动规则制定进程。

努力共建和谐、绿色的网络世界

网络的开放性、跨国性决定了网络安全是全球性挑战，单靠一国之力难以有效应对，必须通过国际合作共同破解这一难题。

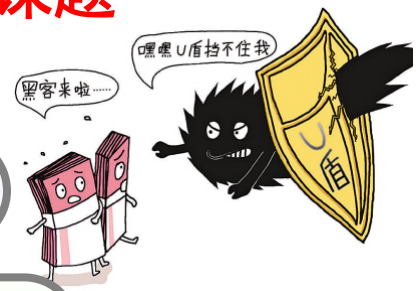


“网络无远近，万里尚为邻”，共同构建一个和谐的绿色的网络世界

- 共同制定网络空间规则
- 深化打击网络犯罪合作
- 加快网络攻防武器关键技术研发
- 完善网络安全对话机制
- 加强全民，特别是对青少年网络安全和道德等教育

网络安全 从我做起

团队有关网络安全与保密通信技术的研究课题



我院网络科学小组安全保密的主要课题

- 混沌保密通信
- 链路数据混沌密码机
- 基于混沌-束晕的网络加密方法
- 数据图形加密技术
- 混沌和网络双结合的网上保密通信

网络安全第一
共同关注！从我做起！