内部资料　　注意保密

山东省教育系统网络安全专题讲座

等级保护相关政策法规解读

山东省信息网络安全协会　　张朝伦

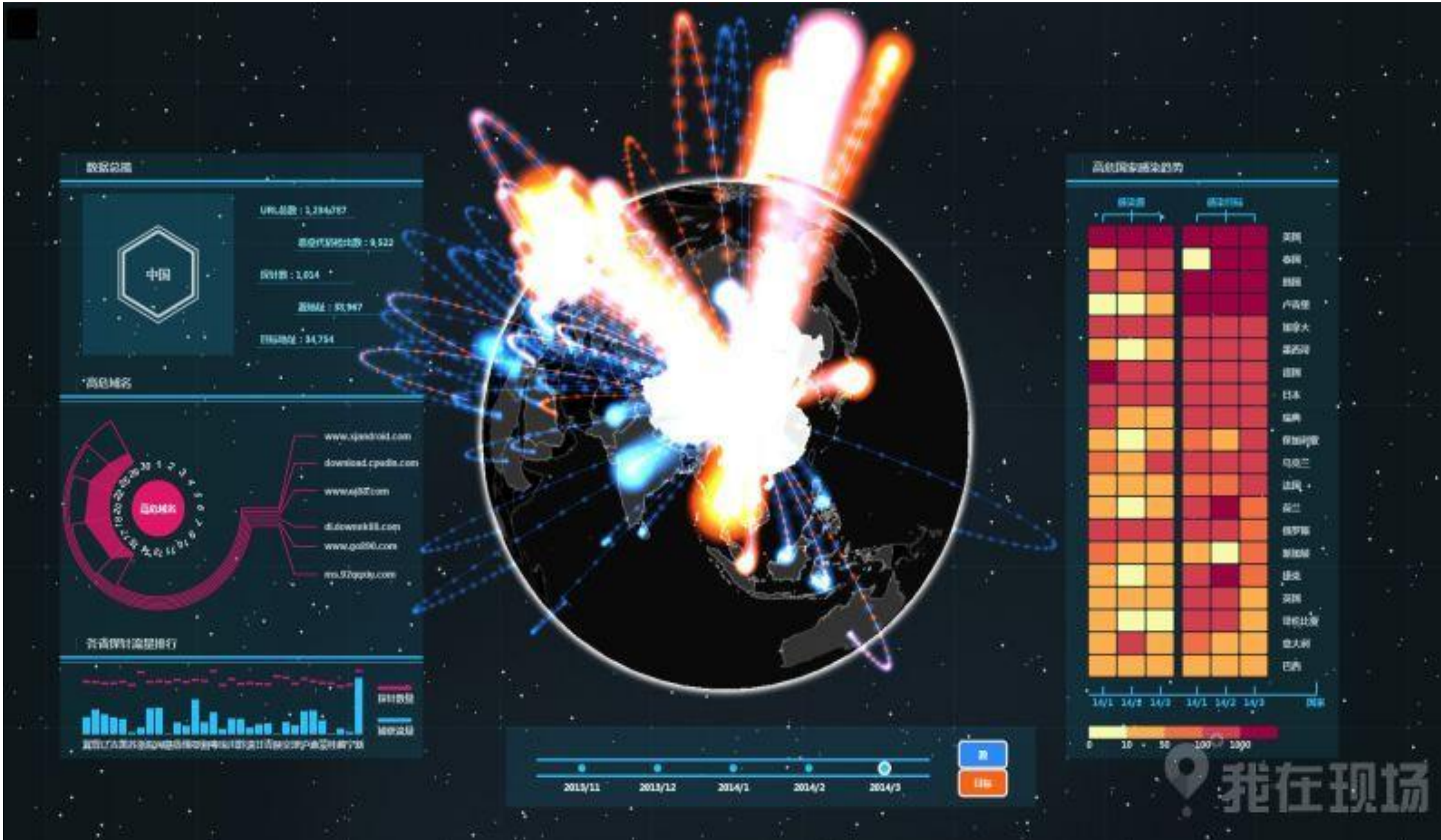
自我介绍

张朝伦

- 公安部信息安全等级保护地方专家组成员
- 公安部信息安全等级保护高级测评师
- 工信部舆情师考试认证中心专家委员会副主任委员
- 能源局山东电力监管办专家组成员
- 山东省信息安全等级保护专家组成员
- 山东省卫生计生系统信息安全技术专家组成员
- 山东省安全生产监督管理局专家成员
- 山东省交通系统等级保护专家组成员
- 山东省统计系统等级保护专家组成员
- 山东省信息网络安全协会副秘书长

- 0531-88366297　　18753145711 微信sdic00
- zclxhx@163.com
- QQ：282773780　　山东省等保群：220491858

课前调查


中国
download.cpadis.com
2013/11
2013/12
2014/1
2014/2
2014/3
我在现场


PASSWORD


信息
安全
等级
保护

为什么积极筹建网络安全实

验室而不愿意落实网络安全

等级保护制度？

邮件门的启示


你瞅我干啥？！
瞅你，咋滴！
汽车之家

特普朗赢了

希拉里载在邮件上

被删除的邮件已恢复


From: Google
Date: March 19, 2016 at 4:34:30 AM EDT
To: john.podesta@gmail.com
Subject: Someone has your password
Google
Someone has your password
Hi John
Someone just used your password to try to sign in to your Google Account john.podesta@gmail.com.
Details:
Saturday, 19 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine
Google stopped this sign-in attempt. You should change your password immediately.
CHANGE PASSWORD
Best,
The Gmail Team


中金网原创
要完！
希拉里刚从“邮件门1.0”中爬出来就跌进了“邮件门2.0”这个坑受此影响希拉里支持率暴跌
反对
支持率
中金网
CNGOLD.COM.CN
中文财经新媒体


360安全中心提醒您
假冒的Google邮
访问真正官网


순sir ㄹ혜
이모
잘 좀
东方IC

邮件门的启示

- 1、不能违纪，更不能违法，违法必被追究，受到法律惩处的时候，上帝也救不了你。
- 2、连美国国务卿的网络环境都能攻破，认为我们的系统安全防护固若金汤的想法，完全是自欺欺人。
- 3、你最相信的伙伴，弄不好就是葬送你前途的杀手。

习总书记4.19讲话对网络空间的见解

- 1.从本体论角度看，网络空间是一种特殊的客观物质存在。
- 2.从认识论角度看，网络实践是人类实践活动的一种崭新样态。
- 3.从唯物史观的角度看，网络空间是人类社会生产力发展的一次新的伟大革命。
- 4.从社会学角度看，网络空间是信息时代人类生活的新领域。
- 5.从国家安全角度看，网络空间是最现实、最复杂、最严峻的安全威胁。

为什么说网络空间是最现实、最复杂、最严峻的安全威胁？

- （1）网络意识形态渗透危机政治安全。
- （2）网络攻击影响经济安全。
- （3）网络有害信息侵蚀文化安全。
- （4）网络恐怖和违法犯罪活动破坏社会安全。
- （5）网络空间军事化威胁国防安全。

- 在当前形势下，
- 网络安全怎么强调都不过分

一、中国信息网络安全立法的发展历程

- 第一部立法是1994年2月18日国务院发布的《计算机信息系统安全保护条例》，之后在计算机系统和互联网安全管理方面又发布了《计算机信息网络国际联网管理暂行规定》、《计算机信息网络国际联网安全保护管理办法》等规范。2000年前后中国互联网服务迅速发展，为规范互联网活动和加强对网络服务提供者的管理，中国颁布了《互联网信息服务管理办法》、《互联网电子公告服务管理规定》、《互联网上网服务营业场所管理条例》等法规和部门规章。

- 在20世纪90年代早期，中国已经出现了计算机犯罪，随着互联网的广泛应用，计算机犯罪发展到网络犯罪阶段。为打击日益严重和不断变化的网络犯罪，1997年中国修订刑法时，规定了非法侵入计算机信息系统罪和破坏计算机信息系统罪两种犯罪，成为最早制定计算机犯罪立法的12个国家之一；

- 2000年12月28日全国人大会常委会通过了《关于维护互联网安全的决定》，明确规定依照刑法有关规定处罚21种利用互联网实施的犯罪；2008年中国重启网络犯罪立法，2009年3月生效的刑法修正案（七）增设了三种新的网络犯罪，以打击新形式的网络经济领域的网络犯罪。中国最高司法机关还为审理新型网络犯罪颁布了若干司法解释。

- 在刑事程序立法方面，2013年生效的新刑事诉讼法明确规定了电子数据证据以及相关的技术侦查措施，标志着中国刑事诉讼法进入了信息化时代。
- 2015年8月29日生效的《刑法修正案（九）》对于《刑法》原来的有关危害计算机信息系统安全规定做了补充和完善，也强化了互联网服务提供者网络安全管理责任，把信息网络上常见的、带有预备实施犯罪性质的行为，在刑法中作为独立的犯罪加以规定，把打击互联网犯罪的节点前移。

- 2015年《中华人民共和国国家安全法》和《中华人民共和国反恐怖主义法》相继通过；2015年7月，作为网络安全基本法的《中华人民共和国网络安全法（草案）》第一次向社会公开征求意见；2016年11月7日，全国人大常委会表决通过了《网络安全法》。立法的迅速推进源自我国面临国内外网络安全形势的客观实际和紧迫需要，标志着我国网络空间法制化进程的实质性展开。

《刑法修正案（九）》
网络安全部分解读

刑法修正案（九）保护网络信息安全五大亮点

- 亮点一：进一步加强对公民个人信息的保护
- 亮点二：明确网络服务提供者履行网络安全管理的义务
- 亮点三：完善网络犯罪的相关规定
- 亮点四：增加编造、传播虚假信息犯罪的规定
- 亮点五：进一步解决举证难问题

亮点一：进一步加强对公民个人信息的保护

- 刑法第二百五十三条之一修改为：
- “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。
- “违反国家有关规定，将在履行职责或者提供服务过程中获得的公民个人信息，出售或者提供给他人的，依照前款的规定从重处罚。
- “窃取或者以其他方法非法获取公民个人信息的，依照第一款的规定处罚。
- “单位犯前三款罪的，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，依照各该款的规定处罚。”

亮点二：明确网络服务提供者履行网络安全管理的义务

- 在刑法第二百八十六条后增加一条，作为第二百八十六条之一：“网络服务提供者不履行法律、行政法规规定的信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，有下列情形之一的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金：
- “(一)致使违法信息大量传播的；
- “(二)致使用户信息泄露，造成严重后果的；
- “(三)致使刑事案件证据灭失，情节严重的；
- “(四)有其他严重情节的。
- “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，依照前款的规定处罚。
- “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。”

亮点三：完善网络犯罪的相关规定

- 在刑法第二百八十七条后增加二条，作为第二百八十七条之一、第二百八十七条之二：
- “第二百八十七条之一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。

亮点三：完善网络犯罪的相关规定

- “第二百八十七条之二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。”

亮点四：增加编造、传播虚假信息犯罪的规定

- 在刑法第二百九十一条之一中增加一款作为第二款：“编造虚假的险情、疫情、灾情、警情，在信息网络或者其他媒体上传播，或者明知是上述虚假信息，故意在信息网络或者其他媒体上传播，严重扰乱社会秩序的，处三年以下有期徒刑、拘役或者管制；造成严重后果的，处三年以上七年以下有期徒刑。”

亮点五：进一步解决举证难问题

- 在刑法第二百四十六条中增加一款作为第三款：“通过信息网络实施第一款规定的行为，被害人向人民法院告诉，但提供证据确有困难的，人民法院可以要求公安机关提供协助。”

焦点一：规定网络服务提供者拒不履行安全管理义务

- 首先，有不履行安全管理义务行为，同时主管部门发出通知后，又有拒不改正这样的主观意愿，最后出现了危害后果，要追究责任。这里提及的“义务”是指关系到网络安全的义务，主要包括信息内容的安全，也包括信息系统本身的安全。

按照刑法规定，构成犯罪的情况，

- 一是致使违法信息大量传播，这是指信息内容安全。如果不履行监管的义务，使违法信息出现在信息网络之上，监管部门已通知采取措施，又拒不采取，造成使违法信息大量扩散传播的后果。

按照刑法规定，构成犯罪的情况

- 二是致使用户信息泄露，这和非法出售、提供公民个人信息相关联衔接。互联网时代，互联网服务提供者会收集、储存大量公民个人信息，一旦信息泄露会给他人人身和财产安全造成威胁。所以必须要管理好信息，如果违反互联网安全管理规定，措施不到位，没有管理好致使信息被泄露，如造成大量客户银行卡信息泄露，大量财产被诈骗、盗窃等情况，构成犯罪。

按照刑法规定，构成犯罪的情况

- 三是致使刑事案件证据灭失，这是指造成社会治安上的损害。如按照互联网信息管理要求，服务提供者要保留客户上网日志等信息和痕迹。如果按照法律行政法规规定的期限和要求保管了就没有问题，如果没有妥善保管，或者将信息删除、毁损等，使得司法机关处理刑事案件时，本来应该有的重要证据灭失，使犯罪无法追究的要追究责任。

焦点二：设立传授犯罪方法通讯群组触犯刑法

- 《刑法修正案（九）》在《刑法》中增加了第287条之一，按照规定，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，进行了明确规定。

- 一是只要有证据证明为实施犯罪在网络上设立了这样的网站、通讯群组的行为，就可以作为犯罪追究。当然，从查处犯罪角度看，侦查机关应当尽可能将整个犯罪链条查清楚。但是如果其他环节无法查清，可以只按这一阶段行为追究。如果已经查清，就要按照具体实施的犯罪行为，以诈骗、贩卖枪支弹药、贩毒等犯罪追究。

- 二是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。比如犯罪分子要卖枪、贩毒，可能不承认这个行为，要按传统犯罪查，就要追查联系他到底把枪卖给谁了，但现在只要发布这样的信息本身就可能构成犯罪。如果确有贩卖行为，就要按相应的犯罪去追究；如果没有相应的证据支持，只能证明他在网站上发布了信息，就按这个追究责任。

- 三是为了实施诈骗等违法犯罪活动，在网上发布信息。与上一种行为不同的是，这种信息从内容上看不是像卖枪、贩毒那样违法性很明显，可能看起来是普通的卖房、卖车等信息，但是行为主体要实施诈骗，目的是要骗别人，这样也可以追究责任。如果最后有一款构成其他犯罪，择一重罪处罚。也就是说，如果不法分子发布了卖毒品等信息，实际上也卖了毒品，就按贩毒处理，而不能按照发布违法犯罪信息处理。

焦点三：为网络犯罪提供技术支持可被独立定罪

- 在《刑法修正案（九）》在《刑法》中增加的第287条之二，对明知他人实施犯罪，提供技术支持或者广告推广、支付结算等帮助行为作出明确规定。

- 明知他人实施犯罪，给他提供互联网接入、服务器托管、网络存储、通讯传输等技术支持，直接便利了犯罪的实施。比如，提供广告推广和支付结算，也是互联网犯罪链条上不可缺少的环节，这些帮助行为使得互联网上相关犯罪行程“社会化分工”，降低了犯罪成本，提高了犯罪效率，增强了罪犯逃避打击的能力。

- 所以，专门对这种帮助行为《刑法》独立作出了规定，如有些人专门帮人去非法获取公民的身份信息用于办理大量银行卡，然后提供转帐、提取现金等的服务，帮助实施互联网诈骗的团伙，收取犯罪收益，逃避打击。这样规定后，如果实施的这些行为都得到查处，即使实施诈骗的人没有抓获，全案没有破获，但是有足够证据证明这个人实施了帮助行为，也可以对其进行独立定罪。

- 当然，该罪的刑罚相对较轻。如果整个案件查清楚后，发现其是整个犯罪集团里专门负责洗钱、转移资金的人员，那就将其作为犯罪集团中重要成员，按相应的犯罪追究。

《网络安全法》部分章节解读

一、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。

二、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。[2]

- 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。

三、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。法律制度设计基本能够涵盖网络安全中的关键控制节点，体系较为完备。除了网络安全等级保护、个人信息保护、违法有害信息处置等成熟的制度规定外，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、国家安全审查制度等都具有相当的前瞻性，成为该法的亮点。从制度具体内容来看，部分规范性内容较为细化，打破了传统“原则性思路”的束缚，具有较强的可操作性。

- 《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。可以看出，一部切合网络安全战略，关注技术、管理与规范的网络安全保障基本法，由十多套（部）配套制度共筑框架的法律体系已悄然成型。

四、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。近年来，世界主要国家和地区都陆续出台了国家层面的关键信息基础设施保护战略、立法和具体的保护方案。以美国为主的西方国家都将关键信息基础设施的保护视为网络安全的最核心部分。

网络安全法获高票通过 明确加强个人信息保护

十二届全国人大常委会第二十四次会议11月7日上午经表决
通过了《中华人民共和国网络安全法》

2015年6月
十二届全国人大常委会第十五次会议对网络安全法草案进行首次审议

2016年6月
十二届全国人大常委会第二十一次会议对网络安全法草案进行第二次审议

2016年10月31日
网络安全法草案提交十二届全国人大常委会第二十四次会议进行第三次审议

网络安全法的出台先后经过了全国人大常委会的三次审议

网络安全法共有7章79条 内容上有6方面突出亮点

1. 明确了网络空间主权的原则
2. 明确了网络产品和服务提供者的安全义务
3. 明确了网络运营者的安全义务
4. 进一步完善了个人信息保护规则
5. 建立了关键信息基础设施安全保护制度
6. 确立了关键信息基础设施重要数据跨境传输的规则

该法自2017年6月1日起施行

新华社发（大巢制图）

- 第五条 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。

- 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。

- 第九条 网络运营者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。
- 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。
- 第十一条 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。

- 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。

- 第六十三条 违反本法第二十七条规定，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。
- 违反本法第二十七条规定，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。

- 第六十五条 关键信息基础设施的运营者违反本法第三十五条规定，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。
- 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。

网络等级保护地位

- 从管理要求上升到法律约束
- 从自愿落实上升到强制执行
- 从工作责任上升到国家义务
- 从行政处罚上升到刑事处罚
- 从管理制度上升到国家战略

不落实等级保护工作的行为

- 1、违法行为；
- 2、冒险行为；
- 3、不负责任行为；
- 4、主动接近刑事处罚的行为；
- 5、拖累别人受罚的行为；

- 麻痹自己的安全意识的同时
- 就开始向监狱的大门迈步

新形势下教育系统网络安全工作重点

教育部办公厅关于开展信息系统安全等级保护工作的通知

教办厅函[2009]80号

各省、自治区、直辖市教育厅（教委），各计划单列市教育局，新疆生产建设兵团教育局，部属各高等学校:

信息系统安全等级保护制度是构建国家信息安全保障体系的基本制度。为进一步做好教育系统信息安全工作，提高教育信息系统安全保障能力和水平，经研究，决定在教育系统全面开展信息系统安全等级保护工作。有关要求通知如下:

一、教育信息系统安全等级保护工作的目标

按[illegible]息系统安全等级保护制度建设的文件

系统全面开展信息系统安全等级保护工作。有关要求通知如下:

一、教育信息系统安全等级保护工作的目标

落实国家有关信息系统安全等级保护制度建设的文件要求，增强各地、各校主管部门领导的信息安全保护意识;开展技术培训，建立信息安全技术队伍，建立健全教育系统信息安全等级保护技术保障体系;全面开展教育系统信息系统的定级、备案和测评工作，对发现的问题及时进行整改，用 3 年左右时间，基本建立教育系统信息系统安全等级保护体系，切实提高教育信息系统安全水平，保证教育信息化的健康持续发展。

二、教育信息系统安全等级保护工作的内容

1.按照国家信息安全等级保护有关要求，对教育系统各

教育部办公厅关于进一步加强网络信息系统安全保障工作的通知

教办厅函〔2011〕83号

各省、自治区、直辖市教育厅（教委），各计划单列市教育局，新疆生产建设兵团教育局，部属各高等学校，部内各司局，各直属单位：

为进一步落实公安部等四部委《关于印发<信息安全等级保护管理办法>的通知》（公通字〔2007〕43号）精神和《教育部2011年工作要点》中“做好教育系统网络信息安全保障工作”的要求，加快建立完备的教育网络信息安全保障体系，现就有关工作通知如下：

一、 加强组织领导，建立健全信息安全管理和责任机制

（一） 各地教育行政部门和学校要高度重视网络信息安全工作，落实责任部门与技术部门，负责网络信息安全的管理与具体实施。各省级教育行政部门、部直属高校和部机关直属单位在2011年10月10日前将填写的《教育系统网络信息安全工作情况表》（见附件）报送至教育部教育管理信息中心（教育信息安全等级保护测评中心）。

（二） 地方各级教育行政部门和学校要制定、完善信息系统安全管理制度；定期进

二、 以信息安全等级保护工作为抓手，建立完善网络信息安全保障体系

各地教育行政部门和学校要按照国家信息安全等级保护制度规定和《教育部办公厅关于开展信息系统安全等级保护工作的通知》（教办厅函〔2009〕80号）要求，开展信息系统定级备案、建设整改和等级测评等各项工作，力争在2012年底基本建立教育信息安全等级保护体系。通过分级建设信息安全等级保护综合管理平台，使等级保护工作常态化、制度化，加强对教育行政部门信息安全等级保护工作的管理。

（一） 落实国家定级备案工作程序，加强教育信息系统定级备案管理。各地教育行政部门和学校要严格按照“自主定级、专家评审、主管部门审批、公安机关审核”的步骤，参照教育信息系统定级有关规范开展定级备案工作。各地教育行政部门和学校要将本单位的信息系统定级结果报主管部门审批。在2011年12月底前，完成所有信息系统的定级备案。

已定级备案但未经上级教育主管部门审批的信息系统，要按照上述程序进行评审及审批。定级不准确的应重新定级和备案。

（二） 开展安全建设整改和等级测评，提高教育信息系统整体安全水平。各地教育行政部门和学校的第二级及以上信息系统，要参照国家和教育行业有关标准规范，在定级备案后2年内完成首次安全建设整改和等级测评工作。已定级的第三级及以上信息系统安全整改方案由教育部组织专家审定，在2012年底前完成首次安全建设整改和等级测评工作。

教 育 部 文 件

教技[2014]4号

教育部关于加强教育行业网络与信息安全工作的指导意见

各省、自治区、直辖市教育厅（教委），各计划单列市教育局，新疆生产建设兵团教育局，有关部门（单位）教育司（局），部属各高等学校，部内各司局，各直属单位：

信息化在促进国家经济和社会发展方面的作用日益凸显，已深

3. 全面实施信息安全等级保护制度。各单位要按照国家和教育部有关信息安全等级保护工作要求，全面实施信息安全等级保护制度。一是要按照教育行业有关规范准确定级和备案，对新建系统要在系统规划、设计阶段同步确定安全保护等级；二是按照国家和教育行业有关标准规范要求进行等级测评，四级系统每年进行两次测评，三级系统每年进行一次测评，二级系统每两年进行一次测评；三是要按照国家和教育行业有关标准规范要求进行安全建设与问题整改，对于新建系统，要在系统设计实施阶段同步建设安全防护措施，对于已建系统要按照系统所定级别进行安全整改。

4. 大力提升网络与信息安全技术防护能力。各单位应研究制定网络与信息安全技术防护方案，建立多层次网络与信息安全技术防护体系，按需配置网络与信息安全防护设备和软件，加强网络与信

信息名称：**教育部办公厅关于印发《教育行业信息系统安全等级保护定级工作指南（试行）》的通知**
信息索引：360A16-99-2014-0013-1　　生成日期：2014-10-29　　发文机构：教育部办公厅
发文字号：教技厅函[2014]74号　　信息类别：其他
内容概述：教育部办公厅印发《教育行业信息系统安全等级保护定级工作指南（试行）》。

教　育　部　办　公　厅

教技厅函[2014]74号

教育部办公厅关于印发《教育行业信息系统安全等级保护定级工作指南（试行）》的通知

各省、自治区、直辖市教育厅（教委），新疆生产建设兵团教育局，有关部门（单位）教育司（局），部属各高等学校，部内各司局、各直属单位：

为进一步加强教育行业信息安全工作，指导和规范教育行业信息系统安全等级保护定级工作，现将《教育行业信息系统安全等级保护定级工作指南（试行）》印发给你们，请结合本地本单位实际，认真组织实施。

教　育　部
公　安　部　文　件

教技[2015]2 号

教育部　公安部关于全面推进教育行业信息安全等级保护工作的通知

各省、自治区、直辖市教育厅（教委）、公安厅（局），新疆生产建设兵团教育局、公安局，有关部门（单位）教育司（局），教育部直

二、工作分工

按照“自主定级、自主保护”的原则，教育行业各单位是信息技术安全工作的责任主体，负责本单位所属信息安全等级保护工作。教育部负责统筹教育行业信息安全等级保护工作，组织教育部内司局、直属单位和部属高校开展信息系统定级、备案、测评和整改。各省级教育行政部门和有关部门（单位）教育司局负责组织本地区教育行业或本部门（单位）所属学校信息安全等级保护工作。公安部加强对教育行业信息安全等级保护工作的监督、检查和指导，地方各级公安机关负责本地区教育机构的信息安全等级保护工作的监督、检查和指导。

建立由教育部、公安部组成的部际协调机制，按照各自职责分工，密切配合，定期沟通和通报工作进展，及时交流备案数据、整改测评情况和检查结果。地方各级教育行政部门、公安机关根据地方实际，建立相应的工作协调机制，及时上报工作进展，保障和促进教育行业信息安全等级保护工作的顺利开展。

教育部办公厅关于成立教育部网络安全和信息化领导小组的通知

各省、自治区、直辖市教育厅（教委），各计划单列市教育局，新疆生产建设兵团教育局，有关部门（单位）教育司（局），部属各高等学校，部内各司局、各直属单位：

为贯彻落实中央关于网络安全和信息化工作的战略部署，切实做好新时期的教育系统网络安全和信息化工作，经研究，决定成立教育部网络安全和信息化领导小组，现将有关事项通知如下：

一、领导小组组成人员

组长：陈宝生 教育部党组书记、部长

副组长：杜占元 教育部党组成员、副部长

成员：教育部有关司局和直属单位（办公厅、政策法规司、发展规划司、人事司、财务司、基础教育一司、基础教育二司、职业教育与成人教育司、高等教育司、教育督导局、民族教育司、教师工作司、思想政治工作司、科学技术司、学位管理与研究生教育司、中央电化教育馆、教育管理信息中心）主要负责同志。

领导小组办公室设在教育部科学技术司，主任由科学技术司主要负责同志担任。

二、领导小组主要职责

贯彻落实中央网络安全和信息化领导小组战略部署，统筹协调教育系统网络安全和信息化重大问题，研究制定教育系统网络安全和信息化发展战略、宏观规划和重大政策。

同时撤销“教育部信息化领导小组”和“教育信息化推进办公室”。

特此通知。

教育部办公厅

2016年10月26日

教育部办公厅关于印发《2016年教育信息化工作要点》的通知

教技厅[2016]1号

各省、自治区、直辖市教育厅（教委），新疆生产建设兵团教育局，部内各司局、各直属单位：

为深入贯彻落实党的十八大及十八届三中、四中、五中全会和习近平总书记系列重要讲话精神，按照第二次全国教育信息化工作电视电话会议的工作部署，我部研究制定了《2016年教育信息化工作要点》，现印发给你们，请结合本地本单位工作实际贯彻执行。

教育部办公厅

2016年2月2日

- （九）推进教育行业网络安全工作。
- 18.加强教育行业信息系统（网站）安全防护。
- 落实《教育部 公安部关于全面推进教育行业信息安全等级保护工作的通知》，基本完成教育行业信息系统（网站）的定级备案和第三级及以上信息系统（网站）的测评整改。（责任单位：科技司、教育管理信息中心、地方各级教育行政部门）
-

- 19.提升教育行业信息技术安全保障能力。
- 按照分级管理、逐级负责的原则，健全信息技术安全通报机制，完善信息技术安全工作管理信息系统，加强对信息技术安全工作的统筹管理。研究制定信息技术安全应急预案。加强对信息系统（网站）的监测和预警能力，开展信息技术安全评估。面向部直属单位、直属高校和各省级教育行政部门的信息技术安全支撑部门负责人开展安全管理和技术培训，计划培训200人。（责任单位：科技司、教育管理信息中心、地方各级教育行政部门）

关于加强网络安全学科建设和人才培养的意见

中网办发文[2016]4号

各省、自治区、直辖市、新疆生产建设兵团党委网络安全和信息化领导小组，中央和国家机关各部委：

党的十八大以来，在以习近平同志为总书记的党中央的坚强领导下，国家网络安全人才建设取得重要进展，全社会网络安全意识明显加强。随着信息化的快速发展，网络安全问题更加突出，对网络安全人才建设不断提出新的要求。网络空间的竞争，归根结底是人才竞争。从总体上看，我国网络安全人才还存在数量缺口较大、能力素质不高、结构不尽合理等问题，与维护国家网络安全、建设网络强国的要求不相适应。网络安全学科建设刚刚起步，迫切需要加大投入力度。为加强网络安全学院学科专业建设和人才培养，经中央网络安全和信息化领导小组同意，提出以下意见。

一、**加快网络安全学科专业和院系建设。**在已设立网络空间安全一级学科的基础上，加强学科专业建设。发挥学科引领和带动作用，加大经费投入，开展高水平科学研究，加强实验室等建设，完善本专科、研究生教育和在职培训网络安全人才培养体系。有条件的高等院校可通过整合、新建等方式建立网络安全学院。通过国家政策引导，发挥各方面积极性，利用好国内外资源，聘请优秀教师，吸收优秀学生，下大功夫、大本钱创建世界一流网络安全学院。

二、**创新网络安全人才培养机制。**鼓励高等院校适度增加相关专业推荐优秀应届本科毕业生免试攻读研究生名

- 1、教育信息化建设必须坚持应用与网络安全同步规划、同步实施。
- 2、各级教育管理部门和教学科研机构必须严格履行国家网络安全法律法规规定的责任和义务。
- 3、正确处理好关键基础设施安全防护和网络安全等级保护、网络安全风险评估之间的关系，全面推进网络安全等级保护工作。
- 4、建立和完善自上而下、纵横结合的信息通报机制，实现网络安全预警和处置信息共享。
- 5、进一步加强专业人才队伍建设，保持知识更新，满足管理和应用安全要求。

- 张朝伦
- 手机：18753145711 微信sdic00
  q q: 282773780
- 山东等保群：
- 1群：220491858
- 2群：201735834
- 3群：149853893
  技术支持 ：刘炳旭 18663776355
- 18678788568
-

谢谢大家

山东省信息网络安全协会　　张朝伦