
# 第三届
# 全国网络与信息安全防护峰会

对话·交流·合作

XDef 2014

# 做好新形势下的网络安全保障工作

张俊兵

公安部网络安全保卫局

对话·交流·合作

# 目 录

# 一、外部威胁越来越严重

**一是来自境外对我关键信息基础设施的控制、攻击和窃密的威胁。**

- 有关国家使用各种方法，利用各种途径对我国家关键信息基础设施进行控制、攻击和窃密。
- 据有关部门抽样监测统计，2013年，我国境内有1500余万台主机被境外木马或僵尸网络控制服务器控制。

## 二是来自敌对势力和黑客组织对我网络安全的威胁

- 近年来境内外敌对势力、敌对组织，通过互联网对我政府网站、基础信息网络、重要信息系统等进行入侵攻击、控制和突破。
- 黑客组织持续攻击我政府网站，篡改网页进行造谣煽动，危害国家安全和社会稳定。

# 二、新挑战越来越严峻

## 一是互联网的快速发展，给我维护网络安全带来严重挑战

- 互联网的快速发展，给我维护国家安全和网络安全带来了严重挑战。如果互联网不能得到很好地控制和保护，将给国家安全和社会公共安全带来严重威胁。
- 美国原国务卿奥尔布赖特宣称：有了互联网，对付中国就有了办法。

## 二是网络违法犯罪活动呈快速增长，给社会稳定带来了重大影响

- 一些传统的犯罪类型也更多地利用和针对互联网实施，网络窃密、网络赌博、网络诈骗、网上盗窃等违法犯罪活动日益突出。
- 不法分子利用各种手段窃取、贩卖公民个人信息，从事各种违法犯罪活动，被窃取贩卖或泄漏的信息涉及金融、教育、医疗、快递等重要部门和行业。

## 三是我国信息化建设中核心技术、产品和服务存在安全隐患

- 重要行业部门的操作系统、数据库、服务器、核心路由器等关键信息产品依赖国外，具有自主知识产权的技术和产品比较缺乏，存在不确定的安全隐患。
- 据有关方面统计，我国有一半以上的重要信息系统选用国外操作系统、数据库和服务器等关键信息产品。

## 四是网络新技术新应用不断出现，给保护网络安全带来新挑战

基于IPv6下一代互联网、物联网、云计算、大数据、移动互联网等新技术正在加快应用到能源、交通、金融等重要行业，推动着我国技术进步和经济发展。

与此同时，随着新技术新应用的到来，关系国计民生的信息网络以及大数据更易成为网络攻击的目标。

# 三、安全问题和隐患越来越突出

## 一是关键信息基础设施安全隐患严重，日益影响国家安全和社会公共安全

我国政府网站和重要信息系统，规模宏大、结构复杂，是我国社会发展、经济建设的基石，但存在重大安全隐患和问题。例如，系统存在漏洞；网络架构存在缺陷；系统设计开发存在隐患；信息系统配置不当等等。

# 二是重点行业网络安全还存在突出问题

行业缺乏在机构设置、人员配备、机制、能力等方面的整体考虑和统筹；缺乏顶层设计和规划，安全保护策略不科学；主动发现能力差。缺乏技术手段，难以发现入侵攻击、窃密、安全隐患和问题；主动防护能力差。等级保护、安全监测、通报预警、应急演练等重点工作不落实。

# 四、近年来公安机关开展的网络安全监管工作情况

## 一是开展网络安全执法大检查。

从2010年开始，公安机关每年组织开展重要信息系统和政府网站安全检查，发现整改了一大批网络安全隐患，有力督促了各重点行业、重要部门网络安全工作的开展，提高了国家基础网络和重要信息系统的安全保护能力，也提高了全社会的网络安全防范意识。

## 二是深入推进信息安全等级保护工作。

健全完善了信息安全等级保护工作的组织领导体制，出台了一系列等级保护所需的政策文件和技术标准，深入开展重要信息系统定级备案、安全测评和建设整改工作，加强重要信息系统安全监管，推动了国家信息安全等级保护制度的贯彻落实。

## 三是对政府网站开展安全技术检测。

公安部组织力量对全国数万个政府网站开展了全面技术检测，发现了一大批政府网站存在的安全漏洞和隐患，针对技术检测发现的问题，各级公安机关向政府网站责任单位发送了《政府网站安全隐患告知书》，及时督促整改，提升政府网站的安全保护能力。

**四是进一步完善国家网络安全通报预警体系建设。**

形成了以国家网络与信息安全信息通报中心为核心，相关部委、央企为成员，以及30多家技术支撑单位组成的国家网络与信息安全信息通报机制。依托通报机制，开展了网络安全通报预警、研判分析和网络安全应急处置等多项重点工作。

## 五是严厉打击网络违法犯罪活动。

开展了打击网络有组织造谣、煽动专项行动，有力遏制了网上谣言泛滥，有力维护了网络秩序。

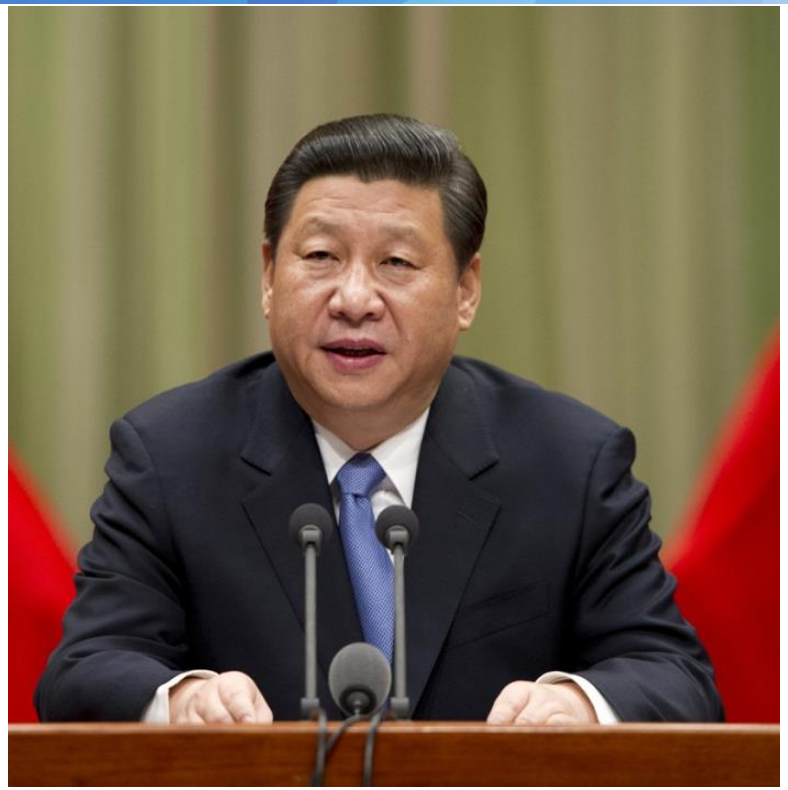
开展了打击网络犯罪专项行动，针对网络攻击、网上盗窃、网络诈骗、网络赌博等违法犯罪活动，破获了一大批案件，抓捕了一大批犯罪嫌疑人，有效保护了网络社会公共安全。

## 六是与发改委、中科院等部门密切配合，组织开展专项和试点示范工作

组织开展了基于IPv6的下一代互联网信息安全专项;重点城市信息化和信息安全示范。

组织开展了下一代互联网信息安全专项产品测试；组织研究起草申报云计算、物联网、工控系统、下一代互联网、移动互联网方面的等级保护系列标准。

# 五、下一步工作打算



今年以来，习近平总书记等中央领导同志对维护我国网络安全作出了一系列重要批示，从全局和战略的高度深刻指出了网络安全问题给我带来的严重威胁和严峻挑战，为我们进一步加强网络空间安全工作，维护国家安全和社会公共安全指明了方向。

2014年2月27日中央成立网络安全和信息化领导小组，召开第一次领导小组会议。习近平总书记在会上指出：“没有网络安全，就没有国家安全。”下一步，要按照中央的统一部署和要求，在中央网络安全和信息化领导小组的统一领导下，充分发挥公安机关的网络安全监管职能作用，全力保障国家网络安全。

## 一是坚持积极防御、综合防范的战略方针。

充分认识网络安全面临的风险和威胁，立足于安全保护、加强预警和应急处置，从更深层次和长远考虑，提高隐患发现、安全保护、应急反应、信息对抗四个能力，坚持预防、监控、应急处理和打击犯罪相结合，做好保护、检测、反应、恢复、预警等环节工作，实现对网络和信息系统的安全可控。

## 二是坚持政府主导、社会参与的原则，充分发挥各方面的积极性。

继续完善和落实“谁主管、谁负责，谁建设、谁负责，谁使用、谁负责，谁经营、谁负责”的网络安全责任制，发挥信息系统主管部门和建设、运营、使用单位以及网络服务商的职能作用，进一步规范网上言论和活动。要增强广大网络用户的法制意识和网络安全防范意识，合理合法使用网络，维护好个人的网络安全。

**三是坚持等级保护、突出重点的原则，着力解决影响我国网络安全的突出问题。**

以等级保护制度为抓手，加强国家基础信息网络和重要信息系统的安全保障，进一步明确重点单位网络安全责任，组织重点行业深入开展以网络安全等级保护为核心的安全防范工作，加强重要信息系统的安全监测预警和应急演练。公安机关要进一步加强对重要信息系统的安全监管，组织开展监督检查，督促重要行业、部门深入开展网络安全防范工作。

**四是力争技术创新、安全可控，为我国网络安全打造坚实基础。**

加强安全可控网络安全核心技术的研发，大力发展基于自主技术的网络安全产业，尽快缩短同发达国家的差距，从根本上摆脱被动局面，提高发现、处置能力，避免灾难性安全事故的发生。

## 五是坚持依法监管的原则，推进网络法制化进程。

贯彻落实十八届四中全会精神，把依法治国基本方略引入网络监管领域，顺应网络发展规律特点，不断健全完善网络安全立法，用法律的手段来规范网络行为，促进网络良性、健康发展。通过法律明确哪些是必须禁止的，哪些是可以放开的，从而创造一个相对宽松的环境，让网民适度表达自己的观点，缓解社会矛盾。

# 谢谢！

# 不足之处请提出批评指正