2013年上半年我国信息安全走势分析与下半年预测

国务院发展研究中心
国际技术经济研究所
陈宝国

引言

世界各国不断加强在网络空间的部署，国际网络空间局势十分紧张，我国信息安全环境日益复杂。上半年，我国多次受到网络攻击方面的无端指责，同时却面临严重的境外网络攻击和监控，移动终端病毒等恶意网络行为大幅攀升，信息安全形势不容乐观。展望下半年，信息安全领域仍将面临诸多挑战。

一、上半年信息安全情况综述

2013年上半年，我国整体信息安全形势并不乐观，暴露出信息技术产品漏洞隐患多、安全防御能力不足、安全保障能力缺乏、安全保障工作滞后等问题，难以有效应对国际网络空间的信息安全挑战。下半年，国际网络空间爆发大规模冲突的风险将进一步加剧，世界各国对网络空间监控行为将进一步加强，引发社会动荡的网络行为也将不断增加，新技术新应用带来的信息安全问题也将更加突出，我国信息安全将面临更大的威胁。

（一）基本特点

1. 基础信息网络运行总体平稳

上半年，我国基础信息网络运行总体平稳，骨干网各项监测指标正常，未发生造成较大影响的基础网络运行故障，未发生重大网络安全事件，但存在一定数量的针对互联网基础设施的拒绝服务攻击事件。近期被曝光的美国国家安全局“棱镜”项目显示，微软、谷歌、思科等企业涉嫌与美国政府合作窃取他国隐私信息，我国基础信息网络面临风险。

（一）基本特点

2. 西方持续热炒“中国网络威胁论”

今年以来，西方国家大肆宣传“中国网络威胁论”，污蔑我国为多起网络攻击事件的发起国，并借此恶化我国际环境，打压我国高科技产业。1月底，美国《华尔街日报》、《纽约时报》、《华盛顿邮报》等几家报纸纷纷发表报道称受到来源于中国的黑客攻击。2月，美国网络安全公司Mandiant发布报告，称近年美国遭受的网络黑客攻击多与中国军方有关。3月，韩国受到大规模网络攻击，西方媒体一致指责中国，但经核实攻击源于欧美多个国家。5月，英国媒体称中国军方曾多次试图窃取英国最先进隐形战斗机的秘密情报。6月，日本情报分析机构称，过去一年日本政府和企业遭受的黑客攻击有60%来自中国。

（一）基本特点

3. 境外网络攻击和监控情况严重

上半年，我国遭受的境外网络攻击和监控在持续加剧。一方面，我国境内大量主机被国外木马或僵尸网络控制。据国家互联网应急中心（CNCERT）统计，2013年1-4月间，境外1.5万多个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主机近350万个，其中位于美国的控制服务器控制了中国境内254万个主机IP地址。境外约有1.4万个IP地址通过植入后门对境内近2.5万个网站实施远程控制。另一方面，我国面临着美国的严密网络监控。6月，美国国家安全局被披露在过去近15年中一直从事侵入中国境内电脑和通讯系统的网络攻击，借此获取有关中国的有价值情报。

（一）基本特点

4. 移动终端病毒等恶意网络行为激增

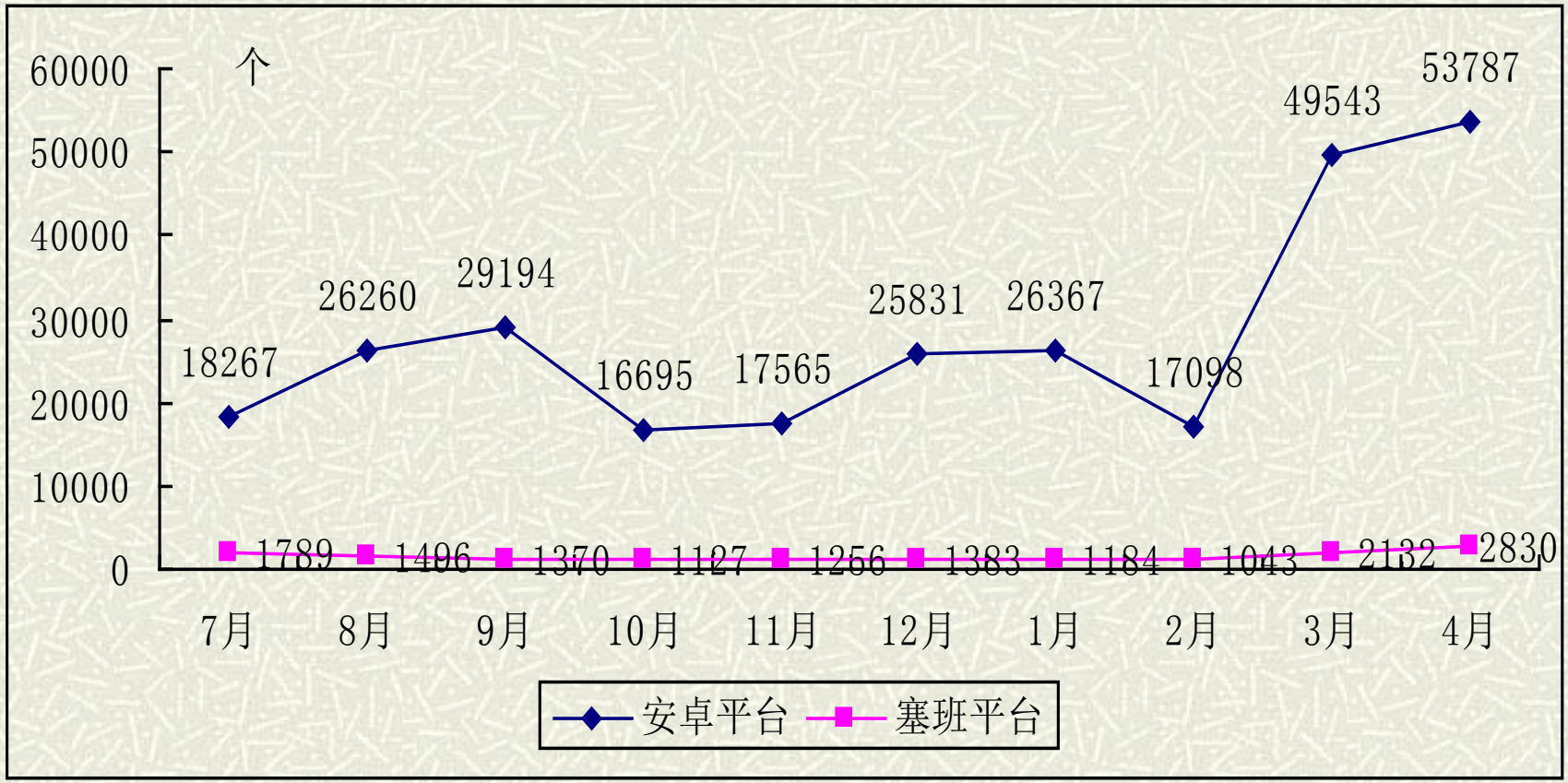
上半年，网站入侵、网络欺诈等恶意网络行为依然呈现上升趋势，特别是移动领域的恶意行为大幅增加。据CNCERT监测，今年1-4月，我国境内被篡改网站数量为35558个，被植入后门的网站数量为31523个，针对境内网站的仿冒页面有12580个。今年1-4月，中国反钓鱼网站联盟共处理钓鱼网站5876个，截止4月，联盟累计认定并处理钓鱼网站108415个。腾讯移动安全实验室的数据显示，今年上半年移动智能终端恶意软件数量激增，如图1所示，特别是3-4月，同比增长超过100%。

（一）基本特点

5. 斯诺登实际持续发酵，全球隐私被美国监控，信任危机冲击互联网安全与合作

- 持续发酵的斯诺登事件源源不断的爆出美国政府监控计划的更多细节。美国当局自“9•11”袭击后，就设立了四大秘密监控计划，其中两个分别取名“明威”和“码头”的项目，负责收集美国人通过电话、外国人通过互联网的讯息交流时间和地点等基本数据，以掌握目标人物的所在地和活动模式。另外两个就直接是收集讯息的内容，其中窃听民众电话的项目叫“核子”，而针对互联网讯息的那个，就正是斯诺登揭露的“棱镜”项目。
- 紧随着美国前中央情报局雇员斯诺登泄露美国安全局监听项目后，德国终止了与英国、美国签署了几十年之久的“信息共享”协议。 。

图1 2012年7月-2013年4月我国移动智能终端恶意软件数量



数据来源：腾迅移动安全实验室，2013年6月

（二）主要问题

1. 信息技术产品漏洞隐患多，被渗透利用的风险高

当前，我国基础信息网络和重要信息系统使用的信息技术产品很多是国外产品，这些产品不可避免地存在安全漏洞。2013年1-5月，中国国家信息安全漏洞库（CNNVD）监测到新增安全漏洞3116个。2013年1-4月，CNNVD共收集信息安全漏洞2601个，并协调处置了238起涉及我国政府部门以及银行、民航等重要信息系统部门及电信、传媒、公共卫生、教育等相关行业的漏洞事件。如，1月Java7被曝出存在远程代码执行零日漏洞，3月域名系统软件BIND 9被曝新增一个拒绝服务漏洞，5月IE8曝出的零日漏洞等。

（二）主要问题

2. 网络空间防御能力不足，难以有效应对大规模网络冲突

我国在网络空间面临严峻的安全形势，但我国网络空间防御能力还存在不足。一方面，我国在网络空间防御方面的技术支撑能力严重不足，在密码破译、战略预警、态势感知、舆情掌控等信息安全核心技术产品上与西方国家还有较大的差距。另一方面，我国信息安全防御力量建设不足，与欧美国家有较大差距。4月联合国裁军研究所的研究数据显示，世界上已经有46个国家成立了网络部队，并持续增加部署，如美国在3月提出要新增40支网络部队。

（二）主要问题

3. 信息安全保障能力缺乏，不能有效保障国家安全

我国信息安全保障能力不足，无力应对国外对我国的网络监控和各类网络安全攻击，不能有效保障国家信息安全。第一，我国信息安全相关技术研发能力严重不足，涉及信息安全核心技术的元器件、芯片等基础产品严重依赖进口，面临严重的安全风险。如近期披露的“棱镜”计划显示，微软、谷歌、思科等数千家科技、金融等领域的企业都与美国政府配合，为其搜集敏感信息。第二，一些关键技术产品的信息安全测评技术缺失。目前我国对进口技术和产品的检测主要集中在功能性测试，很少涉及到其技术核心，不能发现产品的安全漏洞和“后门”。第三，我国信息安全人才严重短缺，而且相比西方国家，缺乏完善的信息安全人才培养体系。

（二）主要问题

4. 信息安全保障工作滞后，管理和防护体系存在漏洞

由于我国与西方国家在技术上存在差距，当前的信息安全保障工作存在一定的滞后性，这给我国信息安全管理和防护带来了安全隐患。一方面，我国缺乏实时追踪国际新技术的机制。我国发现国外新技术信息安全风险，并推出应对措施的时间延迟较大。如国外一些企业推出了“破网技术”，这对我国互联网管理影响较大，而且谷歌近期还推出了提供无线网络的“热气球”，我国尚未对此做出反应。另一方面，我国发现信息技术漏洞与国外存在时间差。很多国外企业与其政府合作密切，往往会优先把发现的漏洞与政府共享，而我国发现的时间往往存在延迟，这就给我国信息安全防护带来了风险。

二、下半年我国信息安全走势分析与预测

（一）全球爆发大规模网络冲突的风险将进一步增加

下半年，国际网络空间的局势将更加复杂，各国会进一步加强网络空间部署，网络冲突也会增多，对我国网络安全形势带来严峻的挑战。随着网络空间的重要性越来越高，世界各国在网络空间的投入都不断加大，国家级网络冲突风险不断增加。第一，世界各国都在加快组建网络部队，网络部队的规模和数量将快速增加。第二，网络空间中与军事相关的行动日益增多，网络摩擦将进一步升级。第三，一些国家间和国家内部已经出现敌对双方的网络冲突，并可能成为导致现实战争的导火索。

二、下半年我国信息安全走势分析与预测

（二）美“网络霸权”思维凸显，大国间“网战”威胁加剧，网络空间规则制定权的博弈激烈展开

美国将国家战略和外交策略中各种不同诉求一并纳入互联网战略,将网络空间视为与陆、海、空、太空并列的行动领域，并与太空、海洋并列的第三大全球公地。美凭借掌控网络战裁定的技术门槛，将网络战和实体战结合起来，确保美军在网络空间开展有效行动。美极力促进欧盟形成“网络安全军事合作战略”，将国际互联网军事化，各国将纷纷建立网络部队以对付来自网络的攻击。

虽然美欧主导网络空间外交局面的格局难以改变，但网络空间法规体系尚未定型，单边、多边竞争与合作、对抗与妥协共存，各国为争取各自利益之间的网络主权斗争已成为2013年下半年全球网络安全的重要内容。

二、下半年我国信息安全走势分析与预测

（三）黑色产业链逐步形成，我信息安全面临重大挑战

下半年，移动终端“黑色产业链”将仍然是网络犯罪的主体，恶意软件或传播手机病毒进行“吸费”行为的黑色产业链，2013年收入将超过10亿元人民币。智能手机、平板电脑等具有强大信息处理能力和网络通信功能的智能移动终端与国民经济运行结合更为紧密。智能移动终端应用更为普及，为用户带来信息失窃、人身安全等多方面安全隐患，手机定位、无线入侵等新兴信息安全问题不断出现。

近期，美国国家安全局的“棱镜”项目曝光，引发国际社会广泛关注。下半年，美国的行为将引发世界各国效仿，各国针对互联网的监控行为将不断加强。美机构针对我国网络监管措施，设立“无线未来计划”、“开放技术计划”“开放网络”等多个项目，研制“混乱技术”、“开放无线基站技术”、“洋葱路由器技术”、“影子互联网技术”等，对我网络监管形成重大挑战。

二、下半年我国信息安全走势分析与预测

（四）新技术新应用带来的信息安全问题将更加突出

随着信息技术的快速发展，新技术新应用层出不穷，云计算、移动互联网、大数据、卫星互联网等领域的新技术新应用带来了新的信息安全问题。第一，云计算本身的安全隐患一直为人所诟病，在广泛应用过程中也经常成为黑客攻击的重要对象。第二，移动互联网得到快速发展，用户数量大大增加，移动设备办公也在企业中广泛应用，而上半年移动领域的安全威胁大幅增长。第三，大数据技术的广泛应用，不仅对信息安全防护提供了新的支撑，而且给我国国家信息安全带来新的挑战，基于大数据技术，一些跨国企业便可以通过在我国收集的大量商业数据分析出涉及国计民生的基础数据，这严重影响到我国经济安全。第四，卫星通信技术在互联网领域的推广应用，将严重影响我国对互联网的有效监管，造成网络舆论的失控，严重影响我国的社会稳定。下半年，云计算、物联网等新技术领域将继续在信息技术领域得到广泛应用，其带来的安全风险将继续对我国信息安全防御体系建设产生影响。

二、下半年我国信息安全走势分析与预测

（五）引发社会动荡的网络行为将不断增加

上半年，国际上多次出现针对网络空间中关键节点的攻击，结果导致了严重社会动荡和经济震荡，其影响十分恶劣。一方面，黑客加强了针对网络媒体的攻击，这可能引发严重的社会恐慌。另一方面，国际上频繁出现金融机构遭受黑客攻击的事件，在社会和经济方面产生的影响日益增加。下半年，受到政治利益或经济利益的驱使，类似能产生重大影响的网络事件还将会频繁出现，相关部门应加强监管。

三、国际信息安全形势

随着信息技术的发展和国际政治、军事斗争形式的变化，信息安全已经成为国家主权的重要组成部分，其重要程度已经超出传统信息化时代信息系统安全的内涵。互联网“接入无线化、业务融合化、终端平板化、数据集中化”的发展趋势对传统的保密制度和信息安全提出了新的挑战，信息安全高端人才成为国际争夺的焦点,网络武器肆孽工控系统，和平时代网络战初现端倪。

三、国际信息安全形势

2013年，国际信息安全形势严峻，信息安全已经成为国家主权被各国予以重视，基于信息安全领域的国际争端不断。美国“网络霸权”愈发凸显，引起了各国的普遍担忧，全球的信息安全形势严峻。

三、国际信息安全形势

- 信息安全已经纳入国家主权被全球广泛关注，下一代网络架构和移动互联网将成为全球争议的焦点
- “网络自由、知识产权、技术标准和信息安全”成为中美网络空间“四大关切”，缺乏互信导致双发实质性合作进展艰难
- 美继续推进“网络霸权”，网络武器大肆泛滥，网络军控被全球广泛关注
- 美重点加强针对中俄的“网络反间”力量，我网络外部环境面临重大挑战
- 跨境高级持续性渗透攻击威胁变化多端，个人隐私成重灾区
- 信息安全人才备受重视，全球人才高端人才竞争备受关注

三、国际信息安全形势

2013年，智慧电网、高速铁路等多基础设施网络融合、急速发展使得我国关键基础设施系统安全前景堪忧。网络安全形势日益严峻，针对我国互联网基础设施和金融、证券、交通、能源、海关、税务、工业、科技等重点行业的联网信息系统的探测、渗透和攻击将逐渐增多。基础信息网络与重要信息系统安全问题普遍存在，支撑国民经济和政务安全运行的能力尚存不足。

三、国际信息安全形势

美继续推进“网络北约”，网络武器大肆泛滥，和平时代的网络战全球广泛关注

当前，现实世界中的双重标准、意识形态和战略竞争等问题正在延伸至网络空间，美国等大国正在加强网络空间的“合纵连横”，致力于构建网络战略同盟。欧洲和日本等发达国家力争与美国合作控制网络空间;北约提出要在北约框架内进行网络“集体防御和攻击”；美在极力促进欧盟形成“网络安全军事合作战略”，并通过制订网络军事防御规范、提供网络安全军事项目援助等手段，试图建立“网络北约”，将国际互联网军事化。

四、工控系统信息安全倍受全球关注

（一）工控系统一直是关键基础实施的重要组成部分

现代工业控制系统包括过程控制、数据采集系统(sCaDa)，分布式控制系统(DCB)，程序逻辑控制(PLC以及其他控制系统等，目前已广泛应用于电力、水力、石化、医药、食品以及汽车、航天等工业领域，成为国家关键基础设施的重要组成部分，其是否能够安全稳定运行，已经关系到国家的战略安全。

四、工控系统信息安全倍受全球关注

（二）新一代信息技术发展为工业控制系统带来机遇的同时，也为工控系统安全带来隐患。

- 物联网
- 云计算
- 移动互联网
- …….

四、工控系统信息安全倍受全球关注

许多工业计算机运行的专有操作系统成为攻击的对象

人们常认为这些计算机比较安全，因为操作人员认为黑客没有兴趣将“恶意代码”植入这些少数系统中。因此，系统中的一些安全漏洞常常不为人所知，很少有人想过如何屏蔽攻击，如何应对现今流行的众多病毒、蠕虫或特洛伊木马。随着工业自动化的发展，过程控制系统与企业信息系统日益紧密结合，国家重要的基础行业（如电力、油气企业等）以及石油化工、制造业的关键控制系统，诸如监控与数据采集系统（SCADA）、可编程序控制器（PLC）、集散控制系统（DCS）、现场总线系统（FCS）和网络控制系统（NCS）遭计算机病毒、“黑客”攻击、信息泄露和认为蓄意破坏等外部威胁的可能性与日俱增。

四、工控系统信息安全倍受全球关注

传统企业信息化与工业控制系统存在诸多的不同

信息化系统的安全措施常常不能够很好地适用于工业控制系统，使得很多关键的控制系统通常处于高风险状态，系统失效所引起的事故时有发生。除了人为地恶意攻击对工业控系统安全造成威胁之外，工业控制系统本身的缺陷也是威胁工业自动化安全的重要因素。

四、工控系统信息安全倍受全球关注

美国政府将颁布专项法律，对关键基础设施供应链实行可视化管理。面对越来越多的基于供应链带来的关键基础设施漏洞和缺陷，美国正在通过一项法律，要求对应用于关键基础设施的所有产品实行全供应链单品可视化跟踪管理和全方位测评。

四、工控系统信息安全倍受全球关注

日本对政府要求对关键基础设施工控系统进行定期对抗模拟和风险评估。通过分析系统的抗风险能力、相关性、脆弱性等，不断提高信息系统的风险防范和快速恢复能力，同时，日本建立了关键基础设施产品进入评测和准入制度，严把入口关。

四、工控系统信息安全倍受全球关注

俄罗斯对关键基础设施装备实行风险评估和强制认证。俄罗斯建有专门关键基础设施装备评估机构和实验室，通过政府文件和强制性标准，对关键基础设施的装备进行强制性风险评估、认证和等级保护。

五、我国工控系统信息安全防范能力较差

与传统的基于TCP/工C协议的网络与信息系统的安全相比，我国工CS的安全保护水平明显偏低，长期以来没有得到关注。我国的工控系统有本征的缺陷，我国的工控系统领域只有面向功能的算法，没有支撑功能的安全算法平台。

五、我国工控系统信息安全防范能力较差

大多数工业控制系统在开发时，由于传统工业控制系统技术的计算资源有限，在设计时只考虑到效率和实时等特性，并未将安全作为一个主要的指标考虑。随着信息化的推动和工业化进程的加速，越来越多的计算机和网络技术应用于工业控制系统，在为工业生产带来极大推动作用的同时，也带来了工CS的安全问题，如木马、病毒、网络攻击造成信息泄露和控制指令篡改等。

六、对我的启示

（一）加强信息安全保障能力建设

- 一是加强信息安全核心技术产品的研发能力。全面推动自主知识产权的芯片、操作系统、可编程控制器等关键技术产品研发，在重点领域启动核心产品的国产化替代。启动对网络攻防技术的研究，分析各项技术的实施细节和表现形式，并提出针对性应对方案。
- 二是加强信息安全防御力量建设。建立成建制的网络部队，成立专门的网络战司令部，全面负责我国网络空间的安全防御。加大信息安全国防投入，培育大量可信赖的信息安全国防承包商和信息安全技术支撑机构，从而提供更尖端的网络技术和工具。
- 三是完善信息安全人才培养体系。制定国家信息安全岗位和职责标准。完善信息安全人才培养和选拔渠道，制定信息安全人才储备计划，保障关键部门信息安全人才需求。

六、对我的启示

（二）注重应对西方国家对我国的网络监控

- 一是加强国家核心数据安全防护工作。明确国外信息技术企业在国内提供产品、技术和服务时的责任和义务，对从事关键行业数据搜集和数据分析业务的企业采取备案制度，避免国外企业对我国互联网的监控。
- 二是建立信息安全态势感知系统。由国家信息安全主管部门牵头，联合国内主要的信息技术企业，实现对网络空间安全态势的监测，感知互联网异动情况，有效分析境外恶意网络行为，及时发现其他国家对我国的网络监控行为。
- 三是启动信息安全核心技术产品的安全检查工作。加强国外进口技术和产品的漏洞分析工作，提升安全隐患的发现能力，促进漏洞信息共享，建立重要领域信息技术、产品及服务的安全检测与审核制度，对进口技术、产品和服务的安全性进行风险评估，有效预防其他国家对我国的网络监控。

六、对我的启示

（三）建立“网络外交”应急响应机制

- 一是启动“网络外交”体制机制建设。针对西方各国频繁污蔑我国为网络攻击的发起国，以及我国遭受严重的网络攻击的现状，我国应建立“网络外交”应急响应小组，积极应对。
- 二是正面应对各国对我国的指责。加强对针对我国的网络攻击的调查取证，并定期发布对调查结果。启动针对西方国家网络攻击指责的应急响应机制，快速分析相关指责或报告的内容，找到其漏洞和问题，形成有实质内容的反馈报告，并予以反击。
- 三是制定国际网络攻击受理流程标准。指定专门的机构受理涉及中国IP网络攻击行为的案件，严格按照中国的法律法规通过标准受理流程处理相关案件。

六、对我的启示

（四）强化对新兴技术的安全防范

- 一是加大对云计算、物联网、移动互联网、卫星互联网等新兴技术研发的资金投入，加强核心技术攻关，提高我国对新兴技术的掌控能力，形成拥有自主知识产权的安全产业链条。
- 二是加快网络防护、入侵检测、身份管理等信息安全关键技术研发，并与新兴技术结合起来，提高新兴技术在应用过程的安全防护能力。
- 三是建立新兴技术的信息安全预警机制，成立专门的机构对新兴技术的信息安全隐患进行分析和研究，并为公众提供相关技术的使用指南或标准，针对关键领域或部门出台强制性标准或规定，限制新兴技术的使用方式和范围。
- 四是针对可能被非法使用的新技术制定应对方案，如针对企图使用卫星互联网绕过国内互联网监管的行为，要加强无线电监听监测和电磁场环境监测，并开发针对性干扰技术。

六、对我的启示

（五）深化与国际社会的合作交流

- 一是加强与世界各国在网络犯罪方面的合作。建立打击国际网络犯罪的机制，在对方能提供证据的情况下积极提供执法调查协助。
- 二是积极参与制订网络空间国际规则。阐明我国对网络敌对行为的态度，强调各国在网络空间的责任和义务，争取在联合国框架下实现国际网络空间的统一管理。
- 三是建立与国际社会的信息安全重大威胁沟通机制，探索建立国家间、地区间应对重大突发事件的信息通报、快速处理的机制，加强信息安全事件应急处理中的交流合作。

六、对我的启示

（六）注重工业控制系统信息安全

- 应尽快制定相关政策，尽快制定“我国关键基础设施工业控制系统信息安全发展规划”和“关键基础设施工控系统信息产品安全管理办法”，将工控系统安全纳入到国家信息安全战略范围予以全面管理。
- 建立关键基础设施工控系统风险评估制度。由工信部信息安全协调司组织专业的第三方机构，对于如国家电网等涉及国计民生的关键基础设施的工控系统，逐步实行定期的风险评估制度，以保证关键基础设施安全稳定运行。

六、对我的启示

（七）强化网络战能力

- 确立“网络防御为主，具备网络还击能力”的网络战略方针。加强我国信息与网络防护，加大资源投入。
- 加速发展网络战相关设施、装备，增强网络抗打击能力，发展网络二次反击能力。
- 以作战需求为牵引，为战而防，消除为防而防、为安全责任而防的消极计算机网络防御思想。