树立安全意识 防范网络侵害

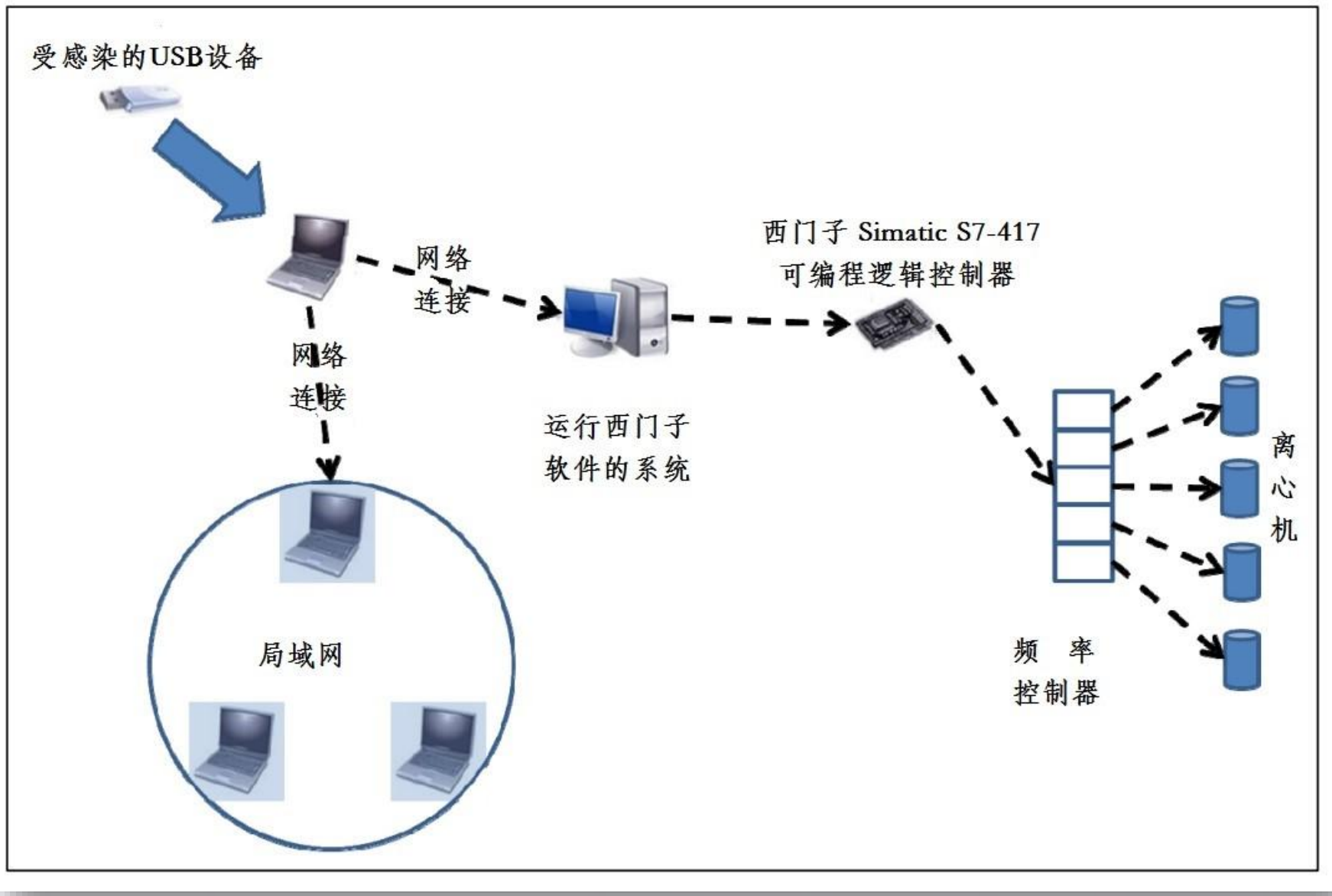
深信服科技 网络安全等级保护专员 尚皓

目录

从几个安全事件说起---震网病毒

震 网 病 毒

从几个安全事件说起---震网病毒



一是让离心机失控;

二是在离心机失控后仍向控制室发出“工作正常”的报告

从几个安全事件说起---深度伪造

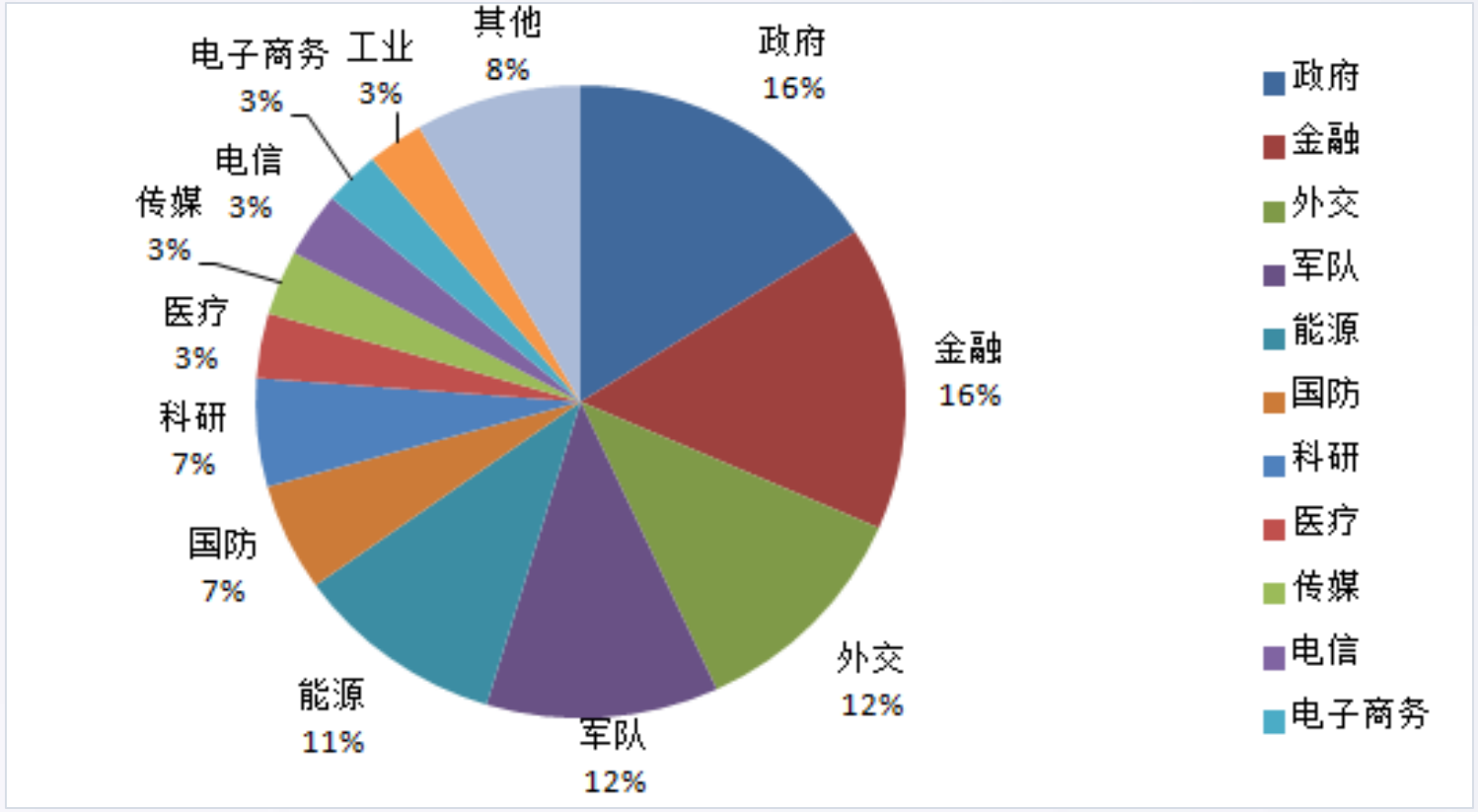
“如果您把用户内容中的人脸换成您或其他人的脸，您同意或确保肖像权利人同意授予“ZAO”及其关联公司全球范围内完全免费、不可撤销、永久、可转授权和可再许可的权利。”

人民网 people.cn

人民网 >> 传媒 >> 最新资讯

人民日报中央厨房：换脸好玩，可不要瞎"ZAO"

网络安全形势---网络环境日趋复杂



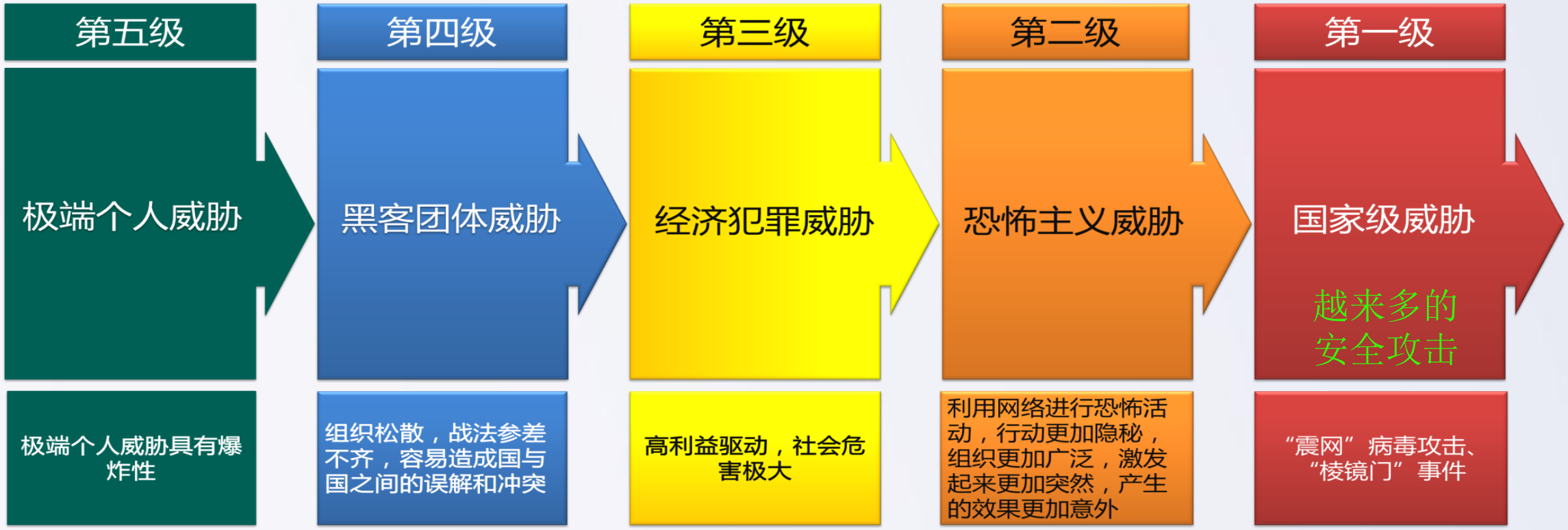
2018年我国面临的高级威胁攻击分别情况

习近平总书记对我国网络安全现状总结：

- 国外垄断网络空间霸权的格局没有根本改变
- 网络空间敌强我弱的态势没有根本改变
- 敌对势力利用网络“扳倒中国”的图谋没有根本改变
- 核心技术受制于人的局面没有根本改变

网络安全形势---网络威胁日益升级

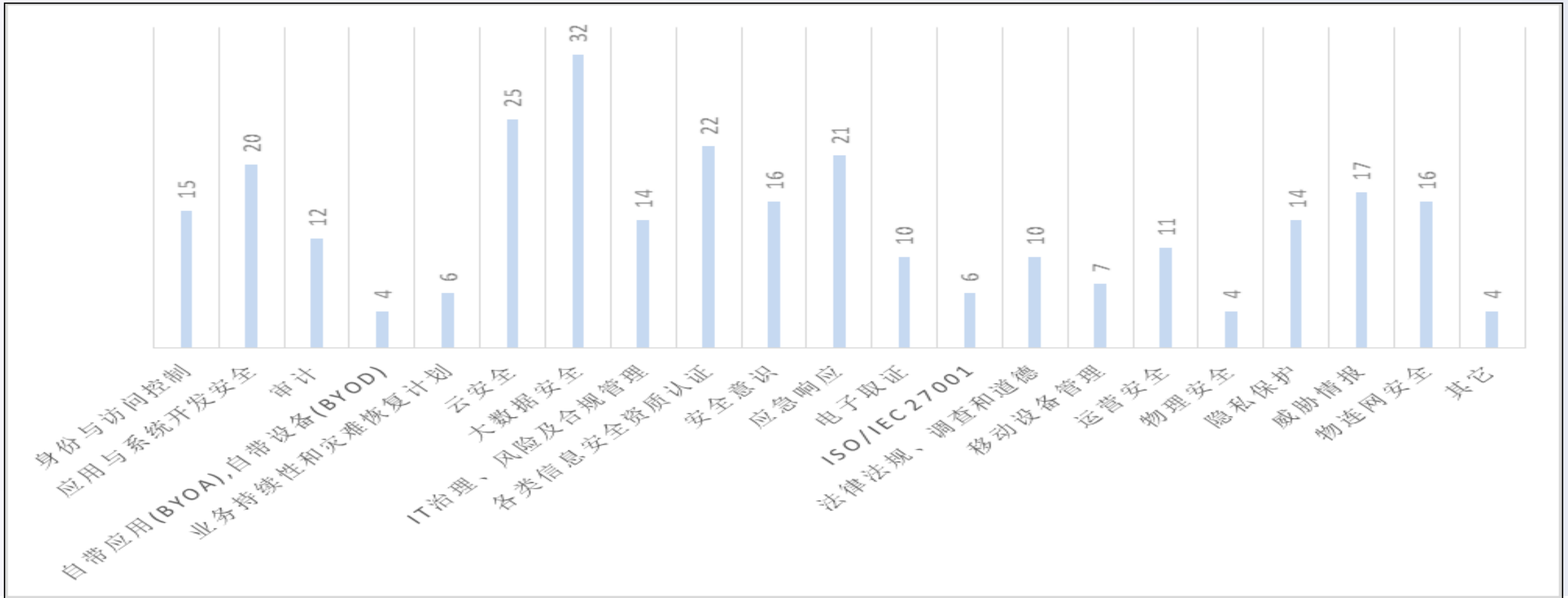
五种威胁严重影响国家安全和经济发展



影响国家安全和经济发展

网络安全形势---网络安全人才匮乏

党的十八大以来，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。



意识形态安全---外部挑战

意识形态安全是指一个国家主体意识形态地位不受任何威胁的相对稳定的状态。无论哪个时代，意识形态问题总是人们关注和争论的焦点，并且是世界历史舞台上的决定性力量之一。

作为和平演变的最重要的手段和武器之一，意识形态是作为推翻国家政权以至改变社会制度的强大舆论力量起作用的。

苏联解体

颜色革命

东欧剧变

意识形态安全---外部挑战

我国20-29岁网民占到网民总数30.4%,是网民占比最高的群体，大学生已经成为我国互联网的主力军之一，当代大学生思想活动上的选择性、差异性、独立性和自由性，以及社会实践的缺乏使得他们的价值取向、思维方式和社会行为更容易受到社会错误思潮的误导和侵蚀，成为美国为首的西方国家进行意识形态渗透的重点

现场！英国知名学者罗思义：西方部分媒体歪曲香港事实真相

意识形态安全---外部挑战

以“棱镜”为代表的美国网络监控体系，打造了美国“知己知彼”的战略优势，服务其网络空间军事行动，确保美国世界“霸主”地位不动摇。

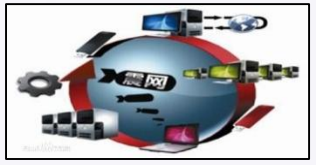
美国政府发布《网络空间国际战略》、《网络空间行动战略》等系列文件，将网络空间纳入美军作战行动领域.

美国相关职能机关

网络窃取及颠覆	网络防卫	网络作战	网络监听
中央情报局	国土安全部	国防部	国家安全局

意识形态安全---外部挑战

一场持续30余年的没有硝烟的战争，巩固了美国的世界霸主地位。



2014 2013 2011 2010 2008

“心脏出血”OPEN SSL
加密的信息未必可靠

“斯诺登”事件
美国利用产业优势监听全球

“茉莉花”革命
网络可以颠覆国家政权

“震网病毒”伊朗
网络攻击毁伤物理设施

“黑屏事件”微软
系统存在不为所控的后门

意识形态安全---外部挑战

美国已经在全球建立了自动的信息
采集、提炼、分析、利用体系

数据

google　思科　facebook

skype　苹果　。。。

利用

分析

提炼

采集

可视化分析平台

Palantir

以“人”为索引组织数据，发现关系；

斯诺登->分析员

搜索引擎

KEYSCORE

“show me all the encrypted word documents form Iran”

搜索来自伊朗的所有加密文档

分析探针

NARUS

全球部署，分析全球30%的网络流量，提炼和关注其关注的“人”的信息

后门设备

CISCO

以思科为代表的网络设备，在国内重要信息系统中占60%以上市场份额

意识形态安全---外部挑战

西方国家利用网络环境制造不利于中国和平发展的舆论环境，主要做法是宣扬“中国威胁论” ，“中国威胁论”使中国在经济、政治、文化等方面在一定程度上损害了中国形象，阻遏了中国的发展步伐。西方国家的“中国威胁论”从实质而言，是西方国家对我国意识形态的进攻。

网络安全关乎国家命运

网络安全关乎你我

目录

国家高度重视网络安全

2014年2月27日，中央网络安全和信息化领导小组成立，习近平任组长。

2016年4月19日，习近平在网信领导小组会上发表重要讲话 -- 4.19讲话。

《网络安全法》实施

2016年12月27日《国家网络空间安全战略》提出9大任务

2017年6月1日《网络安全法》正式实施

《网络安全法》综述

定位

➢是网络安全的基础性法律。

➢是党的十八大以来的又一部重要法律。

制定过程

➢2013年下半年提上日程，2014年形成草案，2015年初形成征求意见稿，2015年6月一审，2016年6月二审、10月31日三审、11月7日人大通过，2017年6月1日起施行。

➢154票赞成、0票反对、1票弃权。

《网络安全法》之责任义务

举报义务和受理责任

第十四条 任何个人和组织有权对危害网络安全的行为向网信、电信、公安等部门举报。收到举报的部门应当及时依法作出处理；不属于本部门职责的，应当及时移送有权处理的部门

有关部门应当对举报人的相关信息予以保密，保护举报人的合法权益。

《网络安全法》之责任义务

网络安全等级保护

国家实行网络安全等级保护制度，并从基本国策上升为法律；

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。

网络与信息安全信息通报中心(市公安局网安支队)接到国家网络与信息安全信息通报中心通报：淮南职业技术学院系统存在高危漏洞，系统存储的4000余名学生身份信息已经造成泄露。

经查，学院未落实网络安全管理制度，未建立网络安全防护技术措施、网络日志留存少于六个月，未采取数据分类、重要数据备份和加密措施，致使系统存储的4353名学生的身份信息泄露。

《网络安全法》之责任义务

个人信息保护

任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。

90后女生杨某在微信上给他人发了四张照片，照片里包含了某小区业主的个人信息，包含房产面积等财产信息，数量达113条。因涉嫌侵犯个人信息罪，杨某在崇州市人民法院受审。最终，法院以侵犯公民个人信息罪判处杨某拘役三个月，缓刑五个月并处罚金4000元。

非法提供公民财产信息
五十条以上即可定罪

《网络安全法》之责任义务

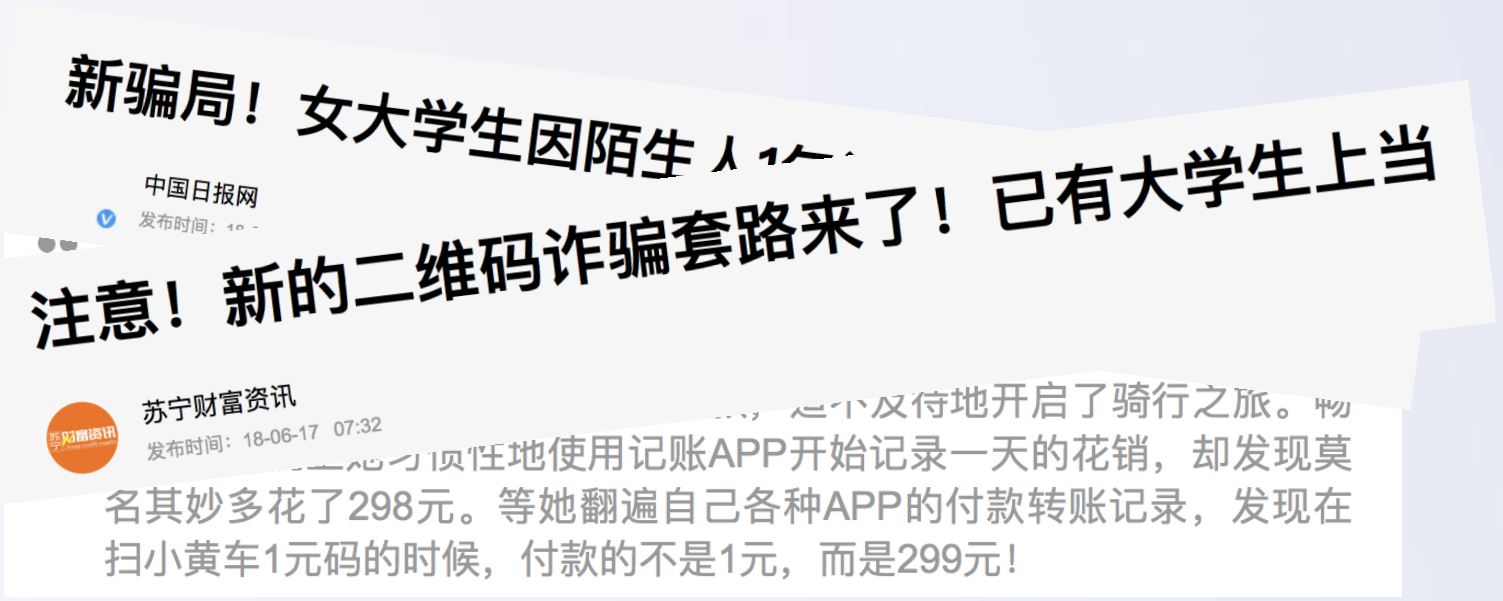
事件应急处置

发生网络安全事件，应当立即启动网络安全事件应急预案，对网络安全事件进行调查和评估，要求网络运营者采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时向社会发布与公众有关的警示信息。

目录

典型安全事件及防护---二维码安全

传统短信验证和新兴二维码扫描方式背后均面临安全风险。2014年通过手机木马劫持支付验证码短信，窃取用户账户信息的活动将呈高发态势。黑客利用手机木马拦截验证码短信，并进一步套取用户网络支付账号和密码，使得用户的个人财产面临巨大损失



> 比如，朋友圈晒扫码领红包、晒扫码领XX产品，骗到你的付款码实现多笔随意刷；比如，后台甩给你一个二维码链接，要求你扫一扫按提示进行操作，结果一扫手机就被植入恶意代码，变成黑灰产的“取款机”……

典型安全事件及防护---伪基站

不需要惊动你

就能转走你的钱

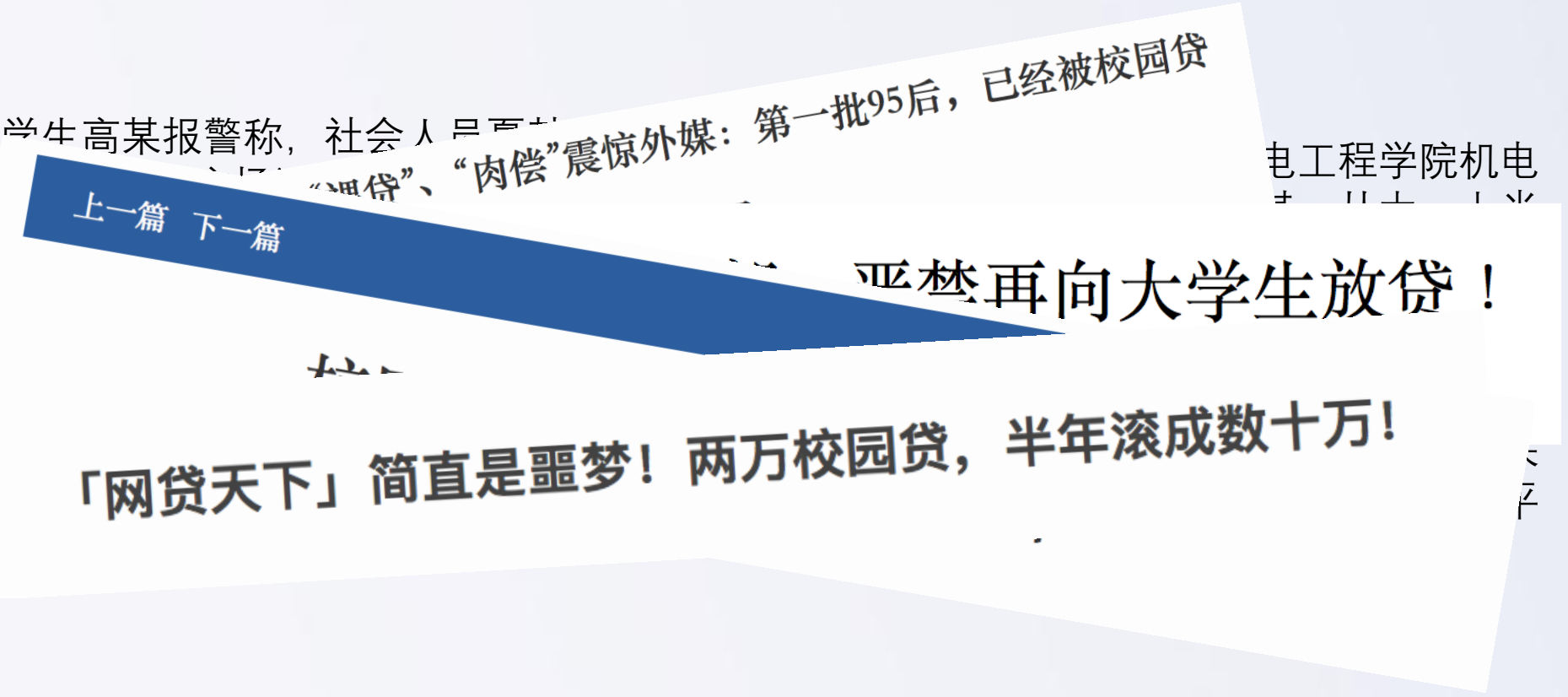
实际上，这是伪基站诈骗的升级版：GSM 劫持 + 短信嗅探 —— 通过伪基站的「GSM 劫持」和「短信嗅探」技术，诈骗人员可以随时劫持你收到或发出的短信。
也许你觉得「伪基站」离自己很遥远，其实伪基站现在几乎散落在大街小巷。最近相信很多人都到过下面的短信，这就是「伪基站诈骗」的基础形式。

典型安全事件及防护---“刷单”兼职

大学生小华看到一则招聘“刷单”兼职的信息：通过虚拟交易帮商家刷销量和信誉，赚取百分之五左右佣金。添加QQ好友后，对方给小华发来一份包括姓名、银行卡号、支付宝账号等信息的申请表。交了申请表，小华开始做“第一单”，对方随即发来一条包含任务编号、购买数量等内容的链接。小华按提示购买了1件商品，支付了100余元。几分钟后，他就收到返款，除本金外还有5元“佣金”。尝到甜头后，小华决定继续“完成任务”。购买、返款，再买、再返……任务不断升级，需要购买的商品数量越来越多。12月29日，当小华支付了一笔8000余元，并完成了“任务”后，客服突然说系统故障，无法返钱，只有重新“刷单”才能一并返款。此时，小华虽然觉得不太对劲，但为了拿回本金，只好照做。果然，再次支付了8000元，继续“刷单”。但是“刷单”之后，他就再也联系不到对方了。

“刷单”本是黑灰色产业，涉嫌欺诈行为，建议同学们不参与，不做此类兼职。切不可贪图小利而落入骗术的圈套。在选择网上兼职工作时，一定要理智，不要被不法分子提出的所谓“高额回报”迷惑。**切忌贪小便宜吃大亏的道理。**

典型安全事件及防护---校园贷



防人之心不可无，不能因为眼前的利益因小失大，特别是在并不了解对方的情况下，不要轻易使用自己的个人信息"帮""替"别人贷款。涉及到金钱，个人信息的事情同学们需要提高万分警惕。

典型安全事件及防护---“直播”骗局

某高校学生小林收到某直播平台发来的私信，称给某主播挂机顶人气就可以轻松挣钱。于是按照对方要求，先交98元注册了一个基础账号，再给对方转账800元，买400个"水军"账号，连同系统赠送的200个"水军"账号，用于给主播顶人气，接着登录网页进行操作，系统提示顶人气的同时会计时，按购买的任务和时间长短返还酬劳，于是小林又转账1280元做任务，对方见小林一步步顺利"入瓮"，又以激活资金为由，诱骗小林继续转账。眼见转账金额越来越大，小林开始怀疑对方身份，想要退出，对方却以放弃任务没有计时不能领取当日工资为由，拒绝小林的退款要求

在进行网游、网购和网赚的时候，不可轻信网页弹出的诱人广告和不明链接，不要透露身份证号、手机号、银行卡号、支付账户及密码等隐私信息，也不要随意扫码，对于主动“打赏”给主播这类事情也需要提高警惕，在直播平台主动送礼物给主播的，期间如并未发生任何诈骗行为，公安机关不一定能受理案件。

典型安全事件及防护---“证件”办理

（1）不要轻易相信网络信息，非正规网站的信息可信度不高；
（2）端正态度，放弃侥幸心理，真实面对考试；
（3）提防网络钓鱼账号，网络聊天时凡要求借钱、还钱，请斟酌账号是否被不法分子所劫持、盗取；
（4）网络账号和绑定的银行借记卡或信用卡一有异常支取，应迅速向网络主体单位反馈信息冻结账号保存证据，并向互联网公安机关报警。
（5）不轻易相信办理各类证书的信息。如需要合格证书，请参加国家相关考试。

典型安全事件及防护---信用卡骗局

王同学用手机上网时，看到一个自称可办理信用卡的网站，其点击链接并输入电话及身份证信息。次日就接到自称信用卡担保方打来的电话，对方先后要王某缴纳500元代办费、2000元激活费、5000元操作费、1万元担保费、1.5万元激活费和3万元其他费用6-7万。半个月后，王同学终于收到了信用卡，但发现是假信用卡。此时，担保方的电话早已关机。

（1）不要轻易泄露个人信息，非正规网站最好不要留下私人信息；
（2）随时更改密码，千年不换的密码安全性很低；
（3）提防钓鱼网站，网络购物时凡要求输入信用卡密码的网站都不是正规的网站；
（4）开通信用卡短信提示功能，有异常应迅速报警。

典型安全事件及防护---“招聘”骗局

李文星求职之死事件：暴露网络求职诈骗“雷区”

中国青年报　2017-08-04 13:41
分享到：

“通过网络招聘平台“BOSS直聘”找工作的东北大学毕业生李文星，最近被发现在天津市静海区溺亡。当地警方根据他随身携带的传销笔记等物证，认为他极有可能误入传销组织。”

网上找工作的骗局有通常有两类：

一类是骗子公司要求职者汇款做为报名费、押金、手续费，凡是这类情况，求职者应当立即放弃，甚至可以举报；

一类是网上传销的骗局，声称只需要交几十元会费就可以在家创业云云，只不过搬到了网上的传销而已。

典型安全事件及防护---“招聘”骗局

李文星求职之死事件：暴露网络求职诈骗“雷区”

中国青年报　2017-08-04 13:41
分享到：

“通过网络招聘平台“BOSS直聘”找工作的东北大学毕业生李文星，最近被发现在天津市静海区溺亡。当地警方根据他随身携带的传销笔记等物证，认为他极有可能误入传销组织。”

网上找工作的骗局有通常有两类：

一类是骗子公司要求职者汇款做为报名费、押金、手续费，凡是这类情况，求职者应当立即放弃，甚至可以举报；

一类是网上传销的骗局，声称只需要交几十元会费就可以在家创业云云，只不过搬到了网上的传销而已。

典型安全事件及防护---“间谍”行动

大连大学生遭台情报机关策反 涉密资料换高额报酬

为赚取报酬，大学生李某某在台谍的指使下，通过到学校图书馆借阅图书等方式，将搜集到的相关资料使用手机拍照后发给对方。台谍还要求李某某想方设法搜集内部、涉密的期刊、学术研究类的成果资料及引荐部队和造船等方面的人员。为达到长期搜情目的，台谍主动引导李某某毕业后到发展潜力较大的军工企业应聘，并承诺其毕业后若进入军工企业，双方可以进行更好的合作。当李某某与沈阳某大型涉密军工企业签订了就业协议书后，台谍表达了长期合作的强烈意愿，并许诺待李某某入职后，每月给予不低于工资的高额报酬。一心期待赚大钱的李某某，最终等来的却是国家安全机关对其的审查。

典型安全事件及防护---计算机安全状态识别

- 计算机运行速度明显变慢
- 操作系统经常提示错误信息
- 一些应用程序打开出现异常
- 在上网过程中不断有广告窗口弹出

- 安装病毒防护程序并及时更新病毒特征库
- 在以下情况注意病毒防范：
- 下载电子邮件附件时；
- 在网络上下载文件时；
- 使用移动存储介质时；
- 安装不明来源的软件时；
- 浏览网页时；
- 计算机使用过程中发现异常时

典型安全事件及防护---用户密码管理

用户名+口令是最简单也最常用的身份认证方式

口令是抵御攻击的第一道防线，防止冒名顶替

口令也是抵御网络攻击的最后一道防线

针对口令的攻击简便易行，口令破解快速有效

中国版25个“弱密码”

*本项统计基于国内流行的密码字典软件破解列表
*标红密码同时也是国外网民常用的“弱密码”

简单数字组合	顺序字符组合	临近字符组合	特殊含义组合
000000	abcdef	123qwe	admin
111111	abcabc	qwerty	password
11111111	abc123	qweasd	p@ssword
112233	a1b2c3		passwd
123123	aaa111		iloveyou
123321			5201314
123456			
12345678			
654321			
666666			
888888			

典型安全事件及防护---网页浏览安全

- 使用安全浏览器（如：搜狗等安全浏览器）
- 收藏经常访问的网站
- 安装杀毒软件，开启实时防护功能，并保持更新；
- 对超低价、超低折扣、中奖等诱惑要提高警惕；
- 警惕色情、赌博、反动等非法网站，避免访问；
- 防止网页自动记住账号密码

网页浏览

典型安全事件及防护---邮件安全

- 应警惕的邮件内容：
  - 你
  - 检
  - 要
- 进
  - 检
  - 近
  - 通
  - 不
  - 在

【重要】IT部第二次异常活动账号提醒-请自行登录系统查看

IT 2018-05-23 17:06
发至 我
详情

你好，IT部门再次拦截到你的外网邮箱近期存在频繁异常活动！请没有登录监控系统查看的同事抓紧登录系统，登录方式采用公司内部的门户登录方式，请登录：http://192.200.200.63:8080/login.php，如果登录系统发现异常请及时联系IT部门!

典型安全事件及防护---介质及环境安全

- 禁止随意放置或丢弃含有敏感信息的纸质文件，废弃文件需用碎纸机粉碎
- 废弃或待修磁介质转交他人时应经管理部门消磁处理
- 离开座位时，应将贵重物品、含有机密信息的资料锁入柜中，并对使用的电脑桌面进行锁屏
- 应将复印或打印的资料及时取走
- UKEY不使用时应及时拔出并妥善保管
- 禁止将手机和无线（例如：360wifi等）连接办公电脑（内网）
- 重要文件存储应先进行加密处理；
- 重要文件通过网络、邮件等方式传输时进行加密处理；
- 开启计算机屏保功能并设置密码，在暂时离开计算机时锁屏幕

SANGFOR
深信服科技

深信服智安全
SANGFOR SECURITY

THANK YOU

2 0 1 9 深 信 服 科 技