国家网络安全宣传周
China Cybersecurity Week

2020

网络安全为人民 网络安全靠人民

国家网络安全宣传周

CHINA CYBERSECURITY WEEK

全民网络安全 知识手册

指导单位：中央网信办

主办单位：北京市委网信办

承办单位：北京市公安局

2020年9月

习近平总书记指出“网络安全和信息化对一个国家很多领域都是牵一发而动全身的，要认清我们面临的形势和任务，充分认识到做好工作的重要性和紧迫性，因势而谋、应势而动、顺势而为”。网络安全事关国家安全和发展，事关广大人民群众切身利益，深刻影响政治、经济、文化、社会、军事等各领域安全。那么，什么是网络安全？如何维护网络安全？政府相关部门采取了哪些措施维护网络安全？本手册将为大家进行专题介绍。

本知识手册分为“法律法规是基础”“系统安全是核心”“网络犯罪是顽疾”“网民行动是重点”四个章节，以期让社会各界和广大市民对网络安全有全面、系统的认知，在日常工作生活中，能够自觉主动、积极行动，共同携手、共同努力维护网络安全。

习近平总书记多次强调：“要抓紧制定立法规划，完善互联网信息内容管理、关键信息基础设施保护等法律法规，依法治理网络空间，维护公民合法权益。”

网络空间与现实社会，并行不悖、相互交织、互相倚重。现实空间有法律等规矩绳墨，网络社会也不可能无法无天、胡作非为。全面推进网络空间法治化，关键词是“法治化”，策略方针是“全面”。

注：曹诗权主编：《2017年新型网络犯罪研究报告》，中国人民公安大学出版社2017年版，第1页。

“互联网立法历程从“无法可循”到“有法可依”

01

传统电信立法期(1994年-2000年)

1 背景

互联网对社会的影响比较有限，当时叫“计算机信息系统”，还没有“互联网”的概念，没有专门的互联网立法，主要解决网络基础设施和网络运行的安全，涉及的都是互联网系统最基本的问题。

2 特点

互联网法律法规“内化”于传统的电信立法中。

1994

1994年2月18日，中华人民共和国国务院令第147号发布《计算机信息系统安全保护条例》

2000

2000年9月25日，中华人民共和国国务院令第291号公布《中华人民共和国电信条例》

2003

2003年5月10日，文化部令第27号发布《互联网文化管理暂行规定》

2005

2005年9月25日，国务院新闻办和信息产业部共同发布《互联网新闻信息服务管理规定》

2007

2007年12月29日，国家广播电影电视总局发布《互联网视听节目服务管理规定》

“互联网立法历程从“无法可循”到“有法可依”

02

互联网法律体系初步建立期(2001年至十八大前)

1 背景

互联网技术及其应用迅猛发展，对经济社会的影响日渐深刻，出现了包括BAT在内的一大批互联网企业。一些专门性的互联网立法出台，涉及互联网新闻信息、互联网营业场所、互联网视听节目等。

2 特点

开始进行专门立法，但分散低位，缺少统筹。立法着眼于信息服务活动，且带有明显的部门特征。

互联网法律体系飞速发展期（十八大-至今）

03

1 背景

互联网对社会的影响进一步加大，既有法律体系不能完全适应发展要求，国家开始着眼于制定一些基础性、全局性、综合性的法律，同时，又不失时机地根据现实发展的要求，出台有针对性的法规。此外，互联网经历大发展大繁荣之后暴露出大量问题，斯诺登事件提醒我们注意到互联网与国家安全的问题；发生在阿拉伯世界的社交媒体革命，使我们意识到了新媒体对社会稳定的影响。

2 特点

加快推动一批基础性、全局性、综合性立法；立法内容从服务业向农业、制造业等全产业辐射。

2013

2013年3月1日，新修订的《信息网络传播权保护条例》正式施行

2015

2015年刑法修正案(九)明确了网络服务提供者履行信息网络安全管理的义务，加大了对信息网络犯罪的刑罚力度，进一步加强了对公民个人信息的保护

2016

2016年11月7日，全国人民代表大会常务委员会发布《中华人民共和国网络安全法》，自2017年6月1日起施行

2018

2018年8月31日，第十三届全国人大常委会第五次会议通过了《电子商务法》

“互联网立法历程从“无法可循”到“有法可依””

@首都网警

互联网法律武器“点点通”

——您生活中可能接触到的互联网法律法规

《关于办理利用信息网络实施诽谤等刑事案件适用法律若干问题的解释》

——网上发言的法律边界

【你问我答】

网上哪些行为属于“捏造事实诽谤他人”？

a、捏造损害他人名誉的事实，在信息网络上散布，或者组织、指使人员在信息网络上散布的；

b、将信息网络上涉及他人的原始信息内容改为损害他人名誉的事实，在信息网络上散布，或者组织、指使人员在信息网络上散布的；

c、明知是捏造的损害他人名誉的事实，在信息网络上散布，情节恶劣的。

2 到何种程度构成诽谤罪（自诉）？

a、同一诽谤信息实际被点击、浏览次数达到五千次以上，或者被转发次数达到五百次以上的；

b、造成被害人或者其近亲属精神失常、自残、自杀等严重后果的；

c、两年内曾因诽谤受过行政处罚，又诽谤他人的；

d、其他情节严重的情形。

3 到何种程度构成诽谤罪（公诉）？

a、引发群体性事件的；　　b、引发公共秩序混乱的；

c、引发民族、宗教冲突的；　　d、诽谤多人，造成恶劣社会影响的；

e、损害国家形象，严重危害国家利益的；　　f、造成恶劣国际影响的；

g、其他严重危害社会秩序和国家利益的情形。

《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》

—— 保护公民个人信息的法律武器

【你问我答】

1 侵犯公民个人信息如何构成犯罪？

- **信息类型和数量**

  基于不同类型公民个人信息的重要程度，分别设置了“五十条以上”“五百条以上”“五千条以上”的入罪标准，以体现罪责刑相适应。

- **违法所得数额**

  违法所得五千元以上。

- **信息用途**

  非法获取、出售或者提供行踪轨迹信息，被他人用于犯罪，知道或者应当知道他人利用公民个人信息实施犯罪，向其出售或者提供。

- **主体身份**

  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。

- **前科情况**

  曾因侵犯公民个人信息受过刑事处罚或者二年内受过行政处罚，又非法获取、出售或者提供公民个人信息的，行为人屡教不改、主观恶性大。

2 企业泄露您的个人信息负什么责任？

网络服务提供者拒不履行法律、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，致使用户的公民个人信息泄露，造成严重后果的，应当依照刑法第二百八十六条之一的规定，以拒不履行信息网络安全管理义务罪定罪处罚。

《网络安全法》

—— 我国第一部网络安全领域专门性综合性立法

【你问我答】

1 法律保护的公民个人信息范围？

公民个人信息是指：以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息，包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等。

《网络安全法》对公民个人信息做了进一步界定，电商、社交、搜索、地图、直播、云及全平台账号密码信息均被纳入公民个人信息范围，并明确了非法获取、出售个人信息等情况的相应处罚措施。

2 您的信息被冒用怎么办？

《网络安全法》特别规定了公民个人信息保护的基本法律制度。通过举报要求网络运营者及时删除被冒用的个人信息，是公民加强个人信息保护的有力武器。

3 您发现危害网络安全的行为可以举报吗？

《网络安全法》明确了公民对危害网络安全行为的举报权利，政府部门有受理、处置公民举报的责任，保障了公民通过网络举报参与网络空间治理的有效性。

《刑法修正案（九）》

——打击整治互联网违法犯罪的“杀手锏”

【你问我答】

1 网络服务提供者拒不履行安全管理义务构成犯罪吗？

- 如果不履行监管的义务，使违法信息出现在网络之上，监管部门通知采取措施，又拒不采取，造成违法信息大量扩散传播的后果，构成犯罪。
- 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。

2 为网络犯罪提供技术支持会被定罪吗？

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。

比如，不法分子帮他人非法获取公民身份信息，用于办理大量银行卡，然后提供转帐、提取现金等服务。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。

习近平总书记指出：“金融、能源、电力、通信、交通等领域的关键信息基础设施是经济社会运行的神经中枢，是网络安全的重中之重，也是可能遭到重点攻击的目标。”

关键信息基础设施

面向公众提供的网络信息服务或支撑能源、交通、水利、金融、公共服务、电子政务、公用事业等重要行业或领域运行的信息系统或工业控制系统。

1. **公众服务类** 如党政机关网站、企事业单位网站、新闻网站等
2. **民生服务类** 如金融、电子政务、公共服务等
3. **基础生产类** 如能源、水利、交通、数据中心、电视广播等

重要网络与信息系统已成为保障城市运转和人们正常生产生活的关键基础设施，这些**信息系统与我们生活息息相关**，一旦遭受攻击破坏，将造成动车出轨、飞机坠毁、地铁对撞追尾、交通信号灯失灵、供电瘫痪等恐怖性灾难。

近年来，针对关键信息基础设施的攻击和破坏活动不断发生。

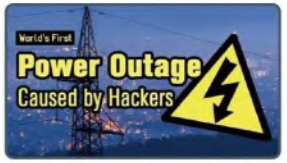
棱镜事件，曝露出各国国家核心数据安全均遭严重威胁

2010 2011 2012 2013 2014

伊朗布什尔核电站遭“震网”病毒攻击，导致核电站数千部离心机被烧毁，放射性物质泄漏

俄乌网络战，导致整个克里米亚地区陆上通讯、移动通信和网络服务被中断

圣诞节前夕乌克兰伊万诺.弗兰科夫斯克州大规模停电，数万“灾民”不得不在严寒中煎熬



2015 2016 2017 2018 **2019**

委内瑞拉停电事件，导致社会严重动荡

这些事件一次次证明关键信息基础设施一旦遭到攻击破坏或数据泄漏，将严重危害国家安全、国计民生、经济发展，这些鲜活的事例也在警示我们，关键信息基础设施安全问题不可一日不防。

关键信息基础设施安全面临严重威胁

关键信息基础设施网络安全隐患风险突出

2019年至今，北京市网络与信息安全信息通报中心共发现全市关键信息基础设施网络系统安全风险点**104**处，安全漏洞**613**个，持续维持高位。相关隐患漏洞一旦被网络攻击渗透，不仅会导致大量核心秘密泄露，更可能造成难以想象的严重后果。同时，我国民航、广电、海关、金融及“水电气热”等关键基础设施的网络设备、系统硬件平台和基础软件有相当部分采用国外产品，关键设备缺乏自主知识产权，并且由于产品性能、系统对接等因素，短时间内难以被国产设备所替代。国外产品的安全性、可控性无法保证，被渗透控制、窃密破坏的风险极高。

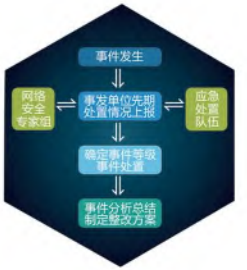
遭受大规模DDOS攻击的风险较大

据《第43次中国互联网络发展状况统计报告》统计，我国约有近**140万**余个IP地址对应的主机被僵尸网络控制服务器所控制，共有**3万**余个IP地址被攻击。从技术角度分析，仅需约**10万**台主机即可造成**100GB**流量的拒绝服务攻击，对重要网络和信息系统造成严重破坏，进而严重影响社会生产生活秩序。近年来，重要行业信息系统遭受DDOS攻击的情况时有发生，成为网络安全防范和风险抵御的突出威胁。

计算机病毒攻击事件频发

2017年，全球爆发了大规模勒索病毒感染事件，我国党政机关、企事业单位内网大规模感染，特别是教育网受损严重，教学系统、校园一卡通系统瘫痪。**2018年**，petya勒索病毒、“永恒之蓝”病毒变种等事件，也对我国互联网带来严重威胁。目前，虽然我国绝大多数党政机关、企事业单位内部网络与互联网隔离。但由于网络安全意识不强，大部分单位内网服务器、电脑未及时更新补丁，存在严重安全隐患漏洞，若办公内网与互联网违规产生数据交互，计算机病毒可直接感染至办公内网，并迅速蔓延扩大造成大面积系统瘫痪、数据恶意加密等，严重影响正常办公秩序，削弱政府和企事业单位社会服务能力。

近年来，北京警方积极思考、主动谋划，立足北京“网都”优势，持续整合各方资源、多方力量，构建了“一个中心，三个支撑”的网络安全态势感知和通报预警工作体系，努力保障首都关键信息基础设施安全稳定运行。



“一个中心”：北京市网络与信息安全信息通报中心
“三个支撑”：动态基础排查、全时监测预警、即时应急处置

“一个中心”和“三个支撑”协调联动，共同对全市重要信息系统和重点网站开展“7X24小时”监测，即时预警网络信息安全隐患漏洞，即时处置各类突发网络信息安全事件。

“一个中心”：北京市网络与信息安全信息通报中心

经过两年磨合试运行，2017年4月，北京市网络与信息安全信息通报中心正式成立，该中心挂靠在市公安局网络安全保卫总队。目前，中心共吸纳成员单位**355**家，覆盖全市各级党政机关、企事业单位、大型互联网企业、网络基础服务公司等网络信息安全重点单位。中心依托**“情况上报、信息共享、预警通报”**三方面工作机制，向成员单位通报网络安全实时动态，并通过手机APP、“平安北京”平台、“首都网警”平台，以及北京电视台、千龙网等媒体向社会大众发布重大突发网络信息安全预警信息，指导帮助成员单位和社会大众防范黑客攻击、病毒侵袭、系统漏洞等网络安全事件。

动态基础排查

大力推进网络安全执法检查常态化运行，动态排查、清除全市信息系统安全隐患。硬化**“隐患问题100%限期整改、重要信息系统100%风险评估、整改效果100%实测验证”**等工作措施，全面实现“问题清零”；对于问题隐患多、无法按期整改的系统，坚决采取**“临时关停、全面断网、人工值守”**等超常规措施，切实做到“风险可控”。

全时监测预警

全面整合社会、公安、等保单位自身等多方监测力量，全时对全市重要信息系统开展实时监测，全时对网页挂马、网站篡改、黑客攻击等网络信息安全突发情况开展实时监测，综合动态、静态网络安全信息，评估风险、发布预警。

即时应急处置

制定出台了《网络安全事件调查处置工作规范》《网络安全事件应急处置预案》，明确职责划分、规范工作流程、健全处置体系，联合科研单位、测评机构、安全厂商组建了**10**支网络安全应急处置队伍，**10**支应急处置技术支撑专家组，**7×24**小时应急值守，强化攻防演练和应急处突能力建设。

信息技术的迅猛发展在极大促进人类文明与进步，为经济社会发展带来勃勃生机和美好愿景的同时，网络犯罪也不期而至，并呈现快速发展蔓延态势。据统计，我国的网络犯罪正以每年30%的速度增长，严重影响广大民众的安全感和经济社会的健康有序发展，成为危害网络安全的顽疾。

30% 每年增速

网络犯罪定义及分类

我国学术界对网络犯罪的界定存在狭义说和广义说两种：

狭义的网络犯罪

指以网络为侵害对象实施的犯罪行为，主要对应我国《刑法》第二百八十五条和第二百八十六条规定的非法侵入计算机信息系统罪和破坏计算机信息系统罪。可简单理解为“**网络作为目标**”。

广义网络犯罪

指利用计算机网络实施的违法犯罪行为。在《刑法》第二百八十五条和第二百八十六条规定的基础上，增加了第二百八十七条等条款，即除了前面所指的“网络作为目标”外，更凸显“**网络作为工具**”。

近年来，传统犯罪借助互联网广泛渗透，“互联网+犯罪”和“犯罪+互联网”交织同构。网络违法犯罪花样繁多，禁而不止、打而不绝，有些网络犯罪甚至呈现出形式多样化、组织团伙化、势力黑恶化、利益链条化、运作产业化、空间国际化等态势，已成为一种新的严重社会公害。其复杂程度、危害程度和泛众化程度远远大于一般传统违法犯罪。

注：曹诗权主编：《2017年新型网络犯罪研究报告》，中国人民公安大学出版社2018年版，第3-4页。

网络犯罪的特点

01
主体年轻多元

据统计，80%的犯罪人员年龄集中18岁至40岁，平均年龄只有23岁。同时，随着计算机技术的发展和网络的普及，各种职业、身份的人都可实施网络犯罪，犯罪主体多元化趋势明显。

02
方式智能专业

网络犯罪作为一种相对高技术犯罪行为，犯罪分子需要掌握基本的计算机操作技能和网络知识，且使用专业犯罪工具实施犯罪，相对传统违法犯罪，方式更加智能专业。

03
类型多样

网络技术的迅速发展普及，给犯罪分子提供了新手段、新工具，诸如网络恐怖主义犯罪、网络虚拟财产犯罪、技术勒索犯罪、妨害流量安全犯罪、网络借贷非法集资犯罪、公民个人信息犯罪、电信网络诈骗犯罪等网络犯罪活动层出不穷，花样繁多。

04
犯罪成本低
作案工具简单

网络犯罪与传统犯罪相比所冒风险小而获益大，其作案工具简单，只需一部联网终端即可实施。作案者只要轻按几下键盘，就可以使被害对象遭受巨大损失。

05
隐蔽性高

互联网打破了时空限制，使得双向、多向交流互动即时、频繁。同时，由于网络具有开放性、匿名性、超越时空性等特点，使得网络犯罪具有极高的隐蔽性、弱关联性，增加了侦破难度。

06
侵害对象广泛

随着社会日趋网络化、扁平化，网络犯罪对象从个人隐私到国家安全，从信用卡密码到军事机密，无所不包，侵害对象广泛。

07
社会危害巨大

网络犯罪的危害性远非一般传统犯罪所能比拟，不仅会造成财产损失，而且会严重危及公共安全和国家安全。目前，从国防、电力到银行、通信等重要信息系统均已数字化、网络化，一旦遭到侵入和破坏，后果不堪设想。

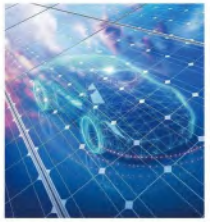
网络犯罪发展趋势

犯罪领域方面

智能家居、工业控制系统、车联网等新兴技术产业将面临严峻的网络安全威胁。

针对大数据、云存储的犯罪活动,由于数据分散且形式多样，犯罪获利大、隐蔽性强,将成为侦查取证的难点。

可穿戴设备、智能医疗设备，在被入侵后甚至可能危害公众的生命，这将彻底颠覆网络犯罪只谋财不害命的观念。



新兴技术产业面临严重威胁

智能家居、工业控制系统、车联网等新兴技术产业将面临严峻的网络安全威胁

大数据、云存储犯罪将多发

针对大数据、云存储的犯罪活动,由于数据分散且形式多样,犯罪获利大、隐蔽性强,将成为侦查取证的难点

智能终端犯罪出现

可穿戴设备、智能医疗设备,在被入侵后甚至可能危害公众的生命

犯罪规模方面

将从单独犯罪转向有组织犯罪。单独的犯罪活动会长期存在，但有组织的犯罪将作为职业和生活方式存在。

犯罪六个方向

黑客组织出租出售“产品”

由黑客组织建立的“僵尸网络”所控制的计算机网络设备被出售或者出租,以用于各种各样的非法目的,包括垃圾邮件、拒绝服务和金融犯罪的木马制作的传播

犯罪工具商业化

黑客工具和Oday漏洞被商业化,可以被公开或者私下贩卖,并提供售后服务

公民隐私商品化

公民隐私成为商品,针对网站攻击并窃取用户信息(爆库和拖库)以供出售成为产业

关键基础设施遭受攻击更为普遍

由黑客组织建立的“僵尸网络”所控制的计算机网络设备被出售或者出租,以用于各种各样的非法目的,包括垃圾邮件、拒绝服务和金融犯罪的木马制作的传播

网络劫持

网络劫持活动越发猖獗

网络黑市

网络“地下黑市”将蓬勃发展

典型网络犯罪

近年来，网络犯罪呈高发态势，据不完全统计，黑客类犯罪、电信网络诈骗类犯罪、侵犯公民个人信息犯罪三类犯罪发案数量占到涉网案件发案总数的90%。为增强打击对称性，北京警方针对以上三类案件开展重点打击。

“净网”专项行动中，在对网络黑色灰色产业为网络诈骗、网络淫秽色情、网络赌博等违法犯罪“输血供电”渠道专项清理整治工作中，共抓获犯罪嫌疑人8000余名，其中可称为黑客的犯罪嫌疑人达1200余名。黑客类犯罪活动猖獗情况可见一斑。目前，黑客类犯罪高发的案件类型有四个方面：

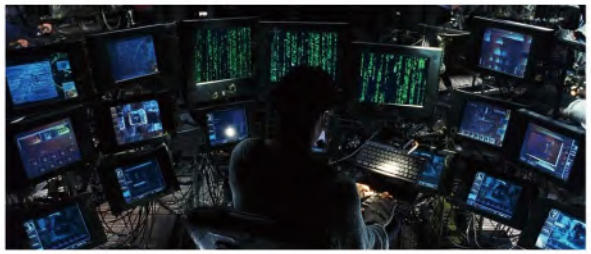
黑客类犯罪

1 非法侵入计算机信息系统案件

此类案件是指“违反国家规定、侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的行为”。

类型 根据权限获取的不同，分为：
内部入侵
网站渗透
木马控制

特点 目标特定、危害性大
非法侵入是行为，而非结果
犯罪隐蔽性强
犯罪动机由争名转向逐利



网上俗称的入侵网站、拖库、销售webshell、僵尸网络等均属于此类犯罪。随着网站数量的不断增多，加之黑客教学组织泛滥，此类违法犯罪的门槛大幅降低，案件数量剧增。

2 非法获取计算机信息系统数据、控制计算机信息系统案件

此类案件是指“侵入国家事务、国防建设、尖端科学技术领域以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处置或者传输的数据，或者对该计算机信息系统实施非法控制，情节严重的行为”。

类型 内部控制
拖库
放置木马等

目的 获取信息系统的控制权
进一步获取数据、放置木马等进行长期控制

此类犯罪系其他三类犯罪的源头性犯罪，社会危害性严重。是公安机关重点打击对象。

3

提供侵入、非法控制计算机信息系统程序、工具案件

此类案件是指"提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具,情节严重的"。

类型

网络攻击类　网络盗号类
网络破解类　手机木马类
游戏外挂类

特点　智能型、匿名性、跨地域性、趋利性、低龄化
专业性、源头性、复合型

此类违法犯罪成本低、且能够带来巨额非法收益，导致屡禁不止、屡打不绝。

4

实施破坏计算机信息系统案件

此类案件是指"违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，或者故意制作、传播计算机病毒等破坏性程序，影响计算机系统的正常运行，后果严重的行为"。

类型

破坏计算机信息系统功能
破坏计算机信息系统数据
修改计算机信息系统应用程序功能
制作传播计算机病毒等破坏性程序
DNS网络劫持

特点　智能型、跨区域性、犯罪成本低、犯罪风险低
人员呈低龄化趋势且有一定的文化水平

典型案例

华中帝国黑客论坛案

黑客工具、教程

8000个

注册会员

2300名

黑客网站

27个

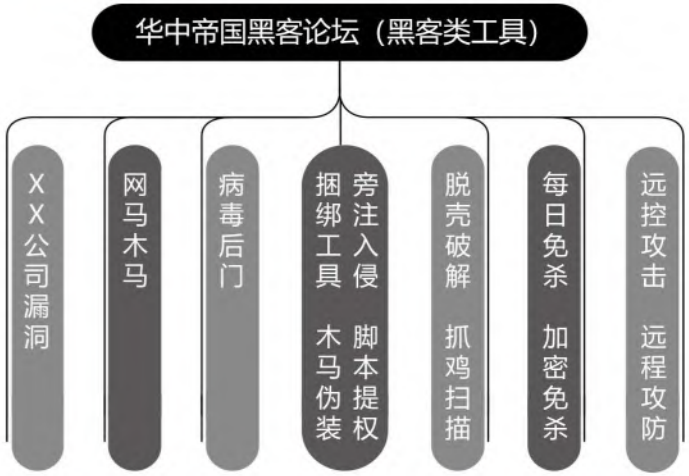
违法有害信息

30000余条

2018年，北京警方在对一黑客网站开展打击时扩线发现，“华中帝国”黑客论坛系多个中小型黑客网站黑客类工具和网络攻击教程的“源头”“上线”，进一步梳理掌握“华中帝国”黑客论坛共发布有黑客类工具、网络攻击教程8000余个，注册收费会员2300余名，是国内设立时间较久、影响较大的黑客网站之一。网站管理者具有较强的反侦察意识，网络行踪诡秘，锁定真实身份困难。

经过对海量数据梳理分析，北京警方最终确定网站管理者为韦某某（男，河南人），并于3月12日将该人抓获，一举将该网络平台摧毁。此后，北京警方持续开展全链条、规模化打击，进一步梳理掌握27个黑客网站，并相继打掉“白蚁网安”“HACK80”“红蓝安全网”等8个会员群体庞大的黑客网站，同时，针对工作发现的黑客类工具、网络攻击教程、黑客网站开展专项清理，共清除违法信息3万余条，斩断了制造、贩卖、传播黑客类工具，并利用黑客类工具危害网络安全的黑色产业链条。

论坛内黑客类工具类型



论坛内容图片

抓捕现场图片

侵犯公民个人信息犯罪

侵犯公民个人信息犯罪是指以窃取或者其他方法非法获取国家机关或者金融、电信、交通、教育、医疗等单位在履行职责或者提供服务过程中获得的公民个人信息，出售或者非法提供给他人，情节严重的行为。

侵犯公民个人信息是电信网络诈骗、敲诈勒索、盗刷信用卡、非法讨债、恶意注册账号等一系列违法犯罪的源头，堪称“百恶之源”。

近年来，公民个人信息被泄露、被非法利用的事件频繁发生，获取公民个人信息的不法分子通过网络建立数据交易平台，大肆出售信息牟取暴利，甚至形成灰色信息产业链，犯罪团伙利用获取的个人信息实施网络诈骗等下游犯罪，严重危害社会安全稳定。

根据犯罪手法划分，侵犯公民个人信息犯罪主要有五类

四个突出特点

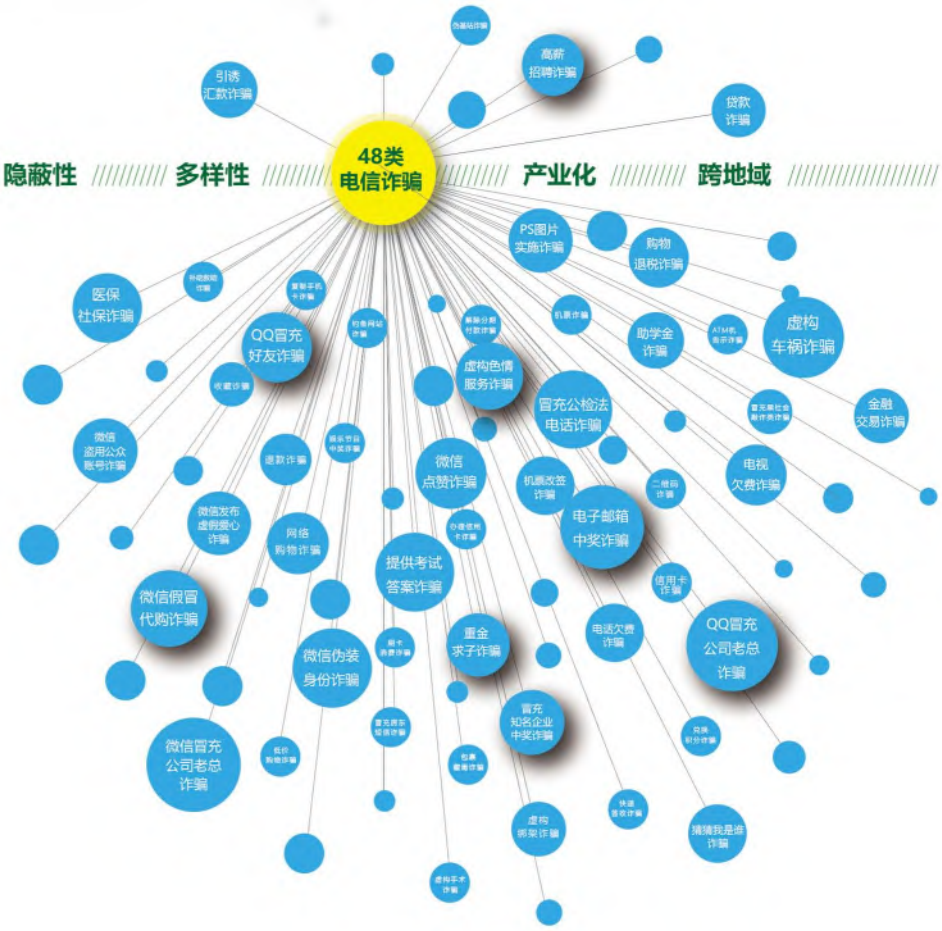
1	犯罪分子获取公民个人信息方式更趋多样
2	互联网、政府机关和金融行业是公民个人信息窃取重灾区
3	行业内部人员和第三方供应商是公民个人信息泄露主要渠道
4	侵害公民个人信息犯罪已经形成完整的产业链条

电信网络诈骗类犯罪

电信网络诈骗是指不法分子通过电话、网络和手机短信，编造虚假信息，利用社会工程学原理设置骗局，对受害人实施远程、非接触式欺骗或直接威胁，骗取受害人利益的一类犯罪手段。

电信网络诈骗是全球经济与通讯一体化带来的必然产物，越来越便捷的通讯和经济往来，使得这类犯罪日益猖獗且呈现全球化趋势。在英美等西方发达国家，电信网络诈骗由于普遍存在而被称为“大众化诈骗”。

近年来，我国电信网络诈骗犯罪持续呈现高发态势，已成为影响社会和国家稳定的突出犯罪问题。犯罪嫌疑人利用民众趋利避害、友情救助等各种心理，通过电话、网络等各类现代通讯工具疯狂实施诈骗，严重危害民众财产安全，扰乱正常生产生活秩序。




案例图

电信网络诈骗流程

网络诈骗流程

目前，电信网络诈骗已形成完整犯罪产业链，按照犯罪流程可分为4个主要环节和15种具体不同的分工

开发制作	钓鱼编辑、木马开发、盗库黑客 不明真相的群众
批发零售	钓鱼零售商、域名贩子、个人信息批发商 银行卡贩子、电话卡贩子、身份证贩子
诈骗实施	电话诈骗 短信代理 在线推广
分赃销售	专业洗钱人、ATM小马仔、分赃中间人



案例图

典型案例

构建虚假网站诈骗案

被骗
2000人

金额
3.3亿

2018年，北京警方接事主范某报警称被欺诈投资黄金损失67万元人民币。北京警方高度重视，迅速组织精干力量开展工作,经缜密侦查，发现谢某某（男，广东人）、王某某（男，四川人）等20名违法犯罪人员，在互联网注册“创盈金银公司”，架设虚假网站“远东贵金属投资平台”，创建QQ群、微信群，以教授股票基础知识为由诱骗网民加入，并分别在网络群组中扮演分析师、投资人、投资助手等不同角色，逐步诱骗网民在虚假网站“远东贵金属投资平台”投资。经梳理，全国被骗事主2000余人，涉案金额高达3.3亿元。2018年6月22日，北京警方在广东珠海将该团伙一举打掉，相关人员被公安机关采取刑事强制措施。

防范提示

如何避免被黑客攻击

- 对关键文件进行加密处理
- 及时更新杀毒软件、安装防火墙，定时查杀手机、电脑病毒上网时开启杀毒软件全部监控
- 定期做好重要资料的备份
- 不要随便打开来源不明的电子邮件
- 在使用移动存储介质之前，先进行病毒查杀之后再安装，禁用系统的自动播放功能
- 上网过程中搜索引擎显示有问题的网页不要打开
- 利用Windows update功能打全系统补丁
- 将应用软件升级到最新版本，其中包括各种即时通讯工具、下载工具和播放器软件、搜索工具条等

如何防护公民个人信息

- 不明链接莫点击
- 快递信息要消除
- 购物办卡需谨慎
- 实名车票要撕毁
- 网络信息隐藏好
- 免费活动有猫腻
- 网站活动少参加
- 微信微博不露财
- 简历管理要妥善
- 网上聊天七不提
- 各类账单保管好
- 复印信息要备注

如何防护电信网络诈骗

- 个人信息不泄露
- 来历不明不轻信
- 核实之前不转账
- 安全软件要安装
- 日常操作要小心

截至2019年6月底，我国网民规模达**8.54亿**

网民数量持续稳居世界**第一**

手机网民规模**8.17亿**

网民每天产生的信息量多达**300亿**条

在互联网迅猛发展的今天，网民一句不良言论，在互联网“聚光灯”“扩音器”效应的影响和助推下，极易产生“雪崩效应”，瞬间引发重大危机事件，不仅严重扰乱正常的网络秩序，更会给现实社会带来巨大的负面影响。网民是网络社会的主体，净化网络生态，构筑清朗的网络空间，离不开每个网民的积极参与和主动行动。

网民规模和互联网普及率

强化认识：持续强化网络安全意识

“患生于所忽，祸起于细微”，没有意识到风险才是最大的风险。在日新月异的互联网时代，网络安全不是“远在天边”，而是“近在眼前”，与我们每个人的工作、学习、生活息息相关。

水、电、气、热、金融等关键基础设施信息系统安全直接影响我们吃住行消乐方方面面，一旦遭受攻击破坏，后果不堪设想。

不法分子持续“开发”“利用”互联网为其违法犯罪“保驾护航”

- **守株待兔**，给网民发送极具诱惑性的钓鱼链接
- **瞒天过海**，给网民发送高仿的货款支付网址
- **糖衣炮弹**，借免费、试用外壳包装病毒木马程序
- **包藏祸心**，打着“高富帅”“白富美”“支教老师”等旗号征友社交诈骗

一旦我们网络安全意识薄弱，好奇心有余、警惕性不足，甚至为贪小便宜，将极易造成我们经济损失甚至危害我们人身安全。

凡事皆有两面性，要一分为二看待互联网“双刃剑”效应，持续强化网络安全意识。只有保持对网络安全的高度敏感敏锐，才能更好迎接互联网给我们带来的红利、福利。

做好自律：自觉约束网络言行，切实做到守法合规

网络社会也是法治社会，网络空间也是公共空间。网络空间和现实社会一样，既提倡、尊重网民交流思想、表达意愿的权利、自由，也依法约束网民的言行，维护良好的网络秩序。我们每名网民在网络上发言不能只图一时痛快，想说什么说什么，想转发什么转发什么，弃法律法规和社会道德于不顾。我们每个网民都有“发声”的自由，但更应有作为网民的基本责任和对网络文明的担当。

网民自律“三不为”

肆意泄愤不可为	01	不要让网络成为一个发泄负面情绪、宣泄负能量的平台
造谣传谣不可为	02	“动荡始于谣言”，谣言不止、社会难安 “谣言止于智者”，不造谣、不信谣、不传谣，自觉抵制阻断谣言传播
盲目跟风不可为	03	保持客观的基础上，对事件进行理性分析、理性发声

主动履责：主动履行公民责任，共同维护网络空间秩序

网络安全同担，网络生活共享。只有每名网民以主人翁的姿态，自觉承担维护网络安全的责任，身体力行地参与到维护网络安全的实际行动中，人人努力、个个担责，网络安全才能坚如磐石、稳如泰山。

市公安局倡议，网民履责要做到“1个主动参与+1个积极加入”，即：主动参与网络社会治理，积极加入首都网警志愿者。

主动参与网络社会治理

监督、举报、报告

持续强化监督、举报，对发现的互联网28类违法有害信息，网络治安乱点乱象，以及信息系统安全隐患漏洞，积极向公安机关等职能部门举报、报告，最大化形成**警民联动、协同共治**的良好局面。

北京市互联网违法和不良信息举报中心
http://www.bjjubao.org/
网络违法犯罪举报网站
http://www.cyberpolice.cn/wfjb/
12321网络不良与垃圾信息举报受理中心
https://www.12321.cn/
“首都网警”微博私信、微信留言

自觉守法、主动宣传

遵守互联网相关法律法规、规章制度要求，积极配合相关部门查处破坏网络秩序的不法人员，主动向身边公众宣传网络安全知识，营造**人人参与网络治理**的良好社会氛围。

履行三个责任

切实担负网络公民的**支持性责任、保护性责任和关怀性责任**，积极为网络治理出谋划策，建言献策；勇于同一切危害网络安全的行为和言论做斗争；充分表达网络公民之间团结互助、关心关爱，共同维护良好的网络空间秩序。

积极加入首都网警志愿者

首都网警志愿者是继“朝阳群众”、“西城大妈”、“海淀网友”、“丰台劝导队”之后的第五支“王牌群众力量”。经过6年的发展，首都网警志愿者队伍已经发展到了6000余人，，累计举报违法犯罪线索9万余条，涉及诈骗、淫秽、色情、网络赌博、吸贩毒、谣言等多个方面。




根据举报，“首都网警”对传播虚假不实、淫秽色情、诈骗等信息的网民4.5万余人进行了警示教育，发布了近万条防范提示类微博、微信，为首都警务工作开展提供了有力支撑。

网警志愿者充分履行公民责任，满怀维护“美丽、干净、安全的互联网家园”的热情，与网警携手合作、群防群治，共同建设和谐文明、健康有序的网络社会。欢迎您加入首都网警志愿者，与我们一起携手、共同维护清朗网络空间。

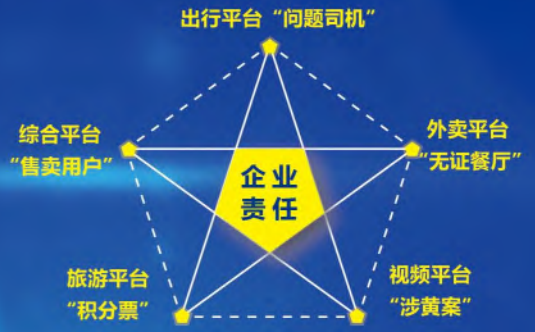
首都网警微博账号

首都网警微信公众号

习近平总书记指出，“要压实互联网企业的主体责任，决不能让互联网成为传播有害信息、造谣生事的平台”。

互联网企业是清朗网络空间建设的主要参与者之一，是维护网络安全的重要一环。互联网企业拥有庞大的用户群体，存储海量网民个人信息，一旦社会责任履行不到位，导致公民个人数据泄漏、违法有害信息泛滥，将对网络社会和现实社会产生严重危害。

同时，随着网络技术的迅猛发展，互联网企业占有的社会资源持续增加，在经济社会中的地位逐步提高，按照权责对等原则，互联网企业应承担更多的社会责任，积极采取措施，规避互联网技术发展中的不利影响，造福社会、服务广大用户。



目前，网络安全、个人信息保护、大数据“杀熟”等企业社会责任议题受到社会广泛关注，各类典型案事例不断出现，严重影响企业发展，更严重扰乱网络空间秩序。

对此，**市公安局倡议：**互联网企业持续提高社会责任意识、增强社会责任感、认真履行社会责任，切实做到恪守法律底线，诚信守法经营；积极传播正能量，大力弘扬社会主义核心价值观；积极参与网络生态治理，努力构建清朗网络空间；自发维护网络和信息安全，履行信息网络安全管理责任；积极参与社会公益事业，促进社会协调发展。

结 语

世界因互联网而更多彩，生活因互联网而更丰富。互联网是我们共同的家园，维护网络安全是我们每个人共同的责任。市公安局倡议：社会各界牢固树立网络社会也是法治社会的理念，主管部门全面履行监管责任，健全完善网络社会治理体系；网络企业自觉履行法律义务和社会责任，配合惩治网络不法行为；网民自觉依法依规约束网上言行，与公安机关一道全面净化网络生态，共建良好网络秩序，让互联网家园更美丽、更干净、更安全。

下一步，北京市公安局将牢牢把握中央＂四个全面＂战略布局、首都＂四个中心＂城市战略定位、公安部＂四项建设＂总体要求，深入践行＂四个第一＂理念，坚持防控风险保安全、服务发展惠民生、改革创新补短板、党建引领铸忠诚，全力提升人民群众的安全感和满意度，推动首都公安＂走前列、创一流＂，为加快京津冀协同发展、建设国际一流的和谐宜居之都做出新的更大的贡献。