

# 2012 年中国互联网违法犯罪问题年度报告

主 办：中国人民公安大学警务改革与发展研究中心

协 办：中国警察网 预防犯罪调查网

课题组组长：魏永忠

课题组成员：（按姓氏笔画排序）

毛欣娟 王新婷 冯文刚 李文君 李伟清 李 侠  
李炜琦 乔 菲 孙 静 吴绍忠 张金菊 张福松  
陈志军 孟 涛 杨 泉 胡一鸣 宋利红 武先江  
赵兴涛 秦 英

2013 年 1 月 18 日

北 京

# 目 录

## 前 言

### 一、2012 年中国互联网违法犯罪概况与特点

#### （一）2012 年中国互联网违法犯罪总体态势

#### （二）2012 年中国互联网违法犯罪主要特点和类型

### 二、2012 年中国互联网违法犯罪问题分类分析

#### （一）网络诈骗：概况、趋势、特点与典型案例

#### （二）网络色情：概况、趋势、特点与典型案例

#### （三）网络赌博：概况、趋势、特点与典型案例

#### （四）网络黑市：制作、复制、传播、贩卖有害信息

#### （五）破坏网络系统安全

#### （六）网络贩毒：概况、趋势、特点与典型案例

#### （七）网络制假售假

#### （八）网络非法交易：（网络黑市、贩卖枪支弹药等）

#### （九）网络恐怖活动

### 三、中国互联网违法犯罪预防对策

#### （一）互联网违法犯罪防治的难点

#### （二）互联网违法犯罪预防治理机制建设

#### （三）互联网违法犯罪防治主要对策

### 四、 中国互联网违法犯罪治理的法治化

#### （一）当前我国在网络安全立法方面面临的问题

(二) 互联网违法犯罪防治的中国法律现状

(三) 互联网违法犯罪防治的境外法治经验

(四) 互联网违法犯罪防治的法治完善建议

结 论

## 前 言

### （一）背景与意义

通过多台计算机、移动通讯设备和信息技术手段联系起来的电子信息互联网络（internet）已日益渗透到人们的日常工作、生活当中，互联网在人们的学习、社交、娱乐、商务等活动中起着越来越不可替代的作用。截至 2012 年 6 月底，中国网民数量已经达到 5.38 亿，互联网普及率为 39.9%。<sup>①</sup>互联网在为人们提供强大服务功能的同时，也成为了一些违法犯罪人员利用的工具，互联网违法犯罪现象近年来有呈现出愈演愈烈的趋势，互联网违法犯罪的类型和形式趋于也趋于多样化、隐蔽化、复杂化。

基于中国互联网上出现的违法犯罪问题，已形成社会危害并显示出当代中国违法犯罪现象的时代特征，我们成立专题学术团队，经过一年的追踪调研、案例收集和深度分析，终于形成《2012 年中国互联网违法犯罪问题年度报告》，旨在引起广大网民、政府相关部门和社会有关方面的关注，为维护网络安全、保护网民的合法权益和社会安全稳定提供有益的参考和借鉴。

### （二）互联网违法犯罪释义

本报告所说的“互联网违法犯罪”是指行为人借助电子信息互联网络实施的危害社会、侵犯他人合法权益的、应受

<sup>①</sup> 中国互联网信息中心《第 30 次中国互联网络发展状况统计报告》，2012 年 7 月 19 日发布

到治安管理处罚或刑事处罚的行为。互联网络既可能成为违法犯罪人员利用的工具，也可能作为违法犯罪的事实场所（如网络泄密、网络侵权等），还可能作为违法犯罪活动侵害的对象（如非法侵入计算机系统等）。本报告所说的互联网违法犯罪包含以上针对计算机网络的违法犯罪，或者以计算机网络作为手段的违法犯罪各种情况，本报告采用的是广义的互联网违法犯罪概念。由于互联网络已经逐渐成为人们沟通日常工具和主要工具，各类违法犯罪行为在实施的过程中都可能在某个环节上利用互联网络来进行，凡是在重要环节、关键环节借助互联网络实施的违法犯罪都是本报告研究的对象，都被认为是“互联网违法犯罪”。

### **（三）互联网违法犯罪类型与特征**

在各类互联网违法犯罪现象中，本报告重点关注的是以互联网络为主要的违法犯罪场所、以非法信息的传递为主要形式的违法犯罪活动。“以互联网络作为违法犯罪场所”是指在“线上”即能完成主要违法犯罪活动的行为，例如网络色情信息传播、网络赌博、网络非法交易、网络泄密、网络侵犯知识产权、部分网络欺诈等，这些违法犯罪行为以“非法传递信息”和“传递非法信息”为主要特征。除此之外的以互联网络为重要工具、但主要在“线下”实施的违法犯罪活动，如利用网络“约会”实施抢劫、强奸等，虽然仍在本报告关注范围之内，但本报告仅对其中数量较大或引起社会较

大反响的违法犯罪情况做出专题报告和分析。

互联网违法犯罪与传统违法犯罪相比，有其独特的特点，虽然互联网违法犯罪侵犯的对象与传统违法犯罪并无不同，但其违法犯罪的形式和手段层出不穷、花样翻新，同时借助互联网络强大的信息传播功能，其违法犯罪的危害可能在极短时间内发生、并且影响巨大。同时，由于互联网违法犯罪行为带有较强的隐蔽性和跨区域性的特点，这给侦破网络违法犯罪的调查取证带来很大障碍，再加上相关法律法规的不健全，使得互联网违法犯罪规模日益增加而治理乏术，互联网违法犯罪的治理已经成为政府和学界关注的重要话题。

#### **（四）互联网违法犯罪治理的困境**

互联网的空间具有全球性、虚拟性和非中心化的特点。网络世界的虚拟性特征，使其没有地域之分，尤其是管辖联系的基础变得模糊不清，这就给网络犯罪的管辖带来难题。

互联网违法犯罪的治理难度主要体现在以下几个方面：一是源头难以控制。越来越多的主体越来越容易的进入互联网络，互联网上可以被利用来进行违法犯罪活动的功能越来越多、越来越复杂。管理者不可能通过限制人、计算机、移动通讯设备的进入或者取消或限制网络功能来控制网络违法犯罪活动，不能因噎废食，因此，可以预见的是，随着互联网络的普及率逐渐提高、互联网各类功能的增加，网络违法犯罪现象在较长的一段时间内仍将处于增涨的趋势。例如

近年来随着互联网络社交功能的日益强大，人们的个人信息在互联网上泄露的可能性在增加，利用这些个人隐私性的信息进行各类诈骗、侵权的活动已经成为互联网违法犯罪活动的重灾区。二是法律依据缺乏。互联网违法犯罪的管辖权，违法犯罪对不特定人群的利益侵犯，违法犯罪行为的认定、取证，新类型的违法和犯罪等问题，都面临着执法依据缺乏的情况。“犯罪”行为的认定较为明确，但许多一般“违法”行为在认定、处罚上都面临着无法可依、无规可依的局面。三是缺乏顶层设计。互联网违法犯罪现象的治理依赖于政府和社会多方的合作，社会管理创新的“党委领导、政府负责、社会协同、公众参与”原则也同样适用于互联网违法犯罪问题的治理。目前，在打击互联网违法犯罪活动中，公安机关仍起着主导作用，但处于单打独斗、疲于应付的状态，势单力薄，尚未形成社会合力。事实上，在预防和打击互联网违法犯罪工作中，政府工信部门、教育部门、宣传部门、互联网接入服务商、内容提供商、科研机构都能发挥各自的作用。提高政府、企业和社会各方对互联网违法犯罪问题的重视，共同为减少互联网违法犯罪献计献策，也是本报告发布的一个重要目的。

#### **（五）《2012 年中国互联网违法犯罪问题年度报告》形成机制**

网络的迅猛发展成为影响当代中国社会、经济、文化、

生活等领域的软力量，与此同时，由于我国网络违法犯罪日趋严重的严峻形势，中国人民公安大学警务改革与发展研究中心于 2012 年 1 月成立专题课题组，组织相关学者和专家专题研究我国的网络犯罪问题，并形成《2012 年中国互联网违法犯罪问题年度报告》，该专题研究报告是我国学界第一次专门针对互联网违法犯罪问题进行的年度综合分析 with 报告，今后将逐年推出。本报告依据公开发表的各类学术资料、新闻报道、政府年鉴及公安机关专项治理成果等资料撰写完成，关注中国互联网 2012 年全年发生的违法犯罪现象，基于互联网上违法犯罪的各类事实进行跟踪观察、总结梳理、个案分析、系统提炼和深度研究是形成本报告逻辑过程。力求信息的真实、可靠、全面，分析客观、简明、精要是本报告形成的目标要求。我们希望本报告能成为学界和政府相关部门在研究或治理互联网违法犯罪问题时的重要参考。

#### **（六）2012 年中国互联网违法犯罪十大类型和十大案件**

课题组在综合分析 2012 年中国互联网违法犯罪问题时认为，对各种违法犯罪现象的社会危害程度和社会公众的关注度有必要做出回应，对 2012 年公安机关全力侦破的典型案件应当给予高度关注。下列两个简表既是 we 分析研究后得出的结论，同样期望对社会有关方面提供积极借鉴。



## 2012 年中国互联网违法犯罪十大类型

排 序	违法犯罪类型	受害者数量	涉案金额	危害度	影响度	总 分
1	网络诈骗	1	2	2	2	7
2	网络色情	2	5	1	1	9
3	网络传销	3	1	3	6	13
4	网络贩卖公民 个人信息	4	6	4	3	17
5	网络钓鱼	5	3	6	5	19
6	网络赌博	7	4	8	8	27
7	网络黑客攻击	9	8	7	4	28
8	网络贩卖假冒 伪劣产品	6	9	10	7	32
9	网络贩毒	10	10	5	9	34
10	网络非法集资	8	7	9	10	34

注释说明：危害度指对社会安全稳定、民众内心的安全感造成损害的程度；影响度指媒体的关注度和该类案件在民众心中的知晓度。

计分说明：

- (1) 按四个指标，即受害者数量、涉案金额、危害度、影响度进行测度。
- (2) 对于每一个指标，都对十类犯罪进行排序。
- (3) 将四个指标的排序累加得到总分，总分最低者综合影响最大，总排序最高。

## 2012 年中国互联网违法犯罪十大案件

编号	案件名称	案件概况
1	<b>“7·19”特大网络贩卖枪支弹药案</b>	公安部直接指挥 29 省区警方集中行动破获“7·19 特大网络贩卖枪支弹药案”，抓获犯罪嫌疑人 530 余名，缴获各类枪支 1000 余支，子弹 1 万余发，以及大量枪支配件。
2	<b>“av 狼”网络传播淫秽色情信息案</b>	新疆警方侦破“av 狼”色情网站案件，注册会员达 100 万，抓获嫌疑人 400 余名。
3	<b>网络诈骗案</b>	福建省福州警方破获利用受害者有过失、不敢报案的心理实施网络诈骗案，受害者涉及全国各省区市 4000 多人，涉案金额达上百万元，警方抓获苏某等 3 名犯罪嫌疑人。
4	<b>网络非法出售公民个人信息案</b>	湖南省长沙警方打掉一个名为“中国资源部”的信息倒卖团伙，犯罪嫌疑人存储的公民姓名、电话、住址、房产、车辆、通话详单、航班记录等数据，总量在 1.5 亿条以上。

5	网络贩卖“盐酸曲马多”毒品案	吉林省警方破获横跨全国 18 个省市、涉案人员达 400 多人的特大网络贩卖精神类药品“盐酸曲马多”案，网络聊天工具、网络交易平台成为贩毒、吸毒者联系主要渠道。
6	特大网络制贩假证、假发票案	辽宁省大连警方抓获利用网络制假贩假犯罪团伙，捣毁制假窝点 6 处，抓获犯罪嫌疑人 19 名，收缴假印章 3 万余枚、各类假证件 15 万余份、假发票 300 余本。
7	攻击、敲诈香港金融业网站案	公安部直接指挥湖南警方摧毁从事网络攻击、实施敲诈的犯罪团伙，抓获肖某等 6 名犯罪嫌疑人。
8	“浮云木马”网银盗窃案	江苏省徐州警方破获将木马程序植入受害人计算机、窃取网银资金案，警方抓获一犯罪团伙嫌疑人 50 余名，涉案金额 1000 余万元。
9	非法获取计算机信息系统数据案	浙江省台州警方破获一犯罪团伙向网游玩家的电脑植入木马盗取游戏账号、装备，作案范围涉及全国 18 个省区市，涉案金额 500 余万元，抓获犯罪嫌疑人 40 余名。

10	<b>“恶意差评师”敲诈勒索案</b>	浙江省杭州警方侦破以给差评为借口向淘宝商家进行勒索案，抓获7名犯罪嫌疑人。
----	---------------------	---------------------------------------

### **（七）2012 年中国互联网违法犯罪重大警情数据**

**数据一：**2012 年，全国公安机关累计破获涉网违法犯罪案件 11.8 万余起，抓获犯罪嫌疑人 21.6 万余人，清理涉枪、涉毒、淫秽色情等违法信息 572 万余条，依法关闭网站（栏目）8 万余个，整治互联网服务单位 2.6 万余家，关停违法网络帐号和通信码号 1.1 万余个。

**数据二：**据赛门铁克公司 2012 年 9 月发布的诺顿安全报告估算，2011 年 7 月至 2012 年 7 月，中国有超过 2.57 亿人成为网络违法犯罪的受害者，平均每天有近 70 万名中国网民遭受不同程度的网络违法犯罪的侵害；网络违法犯罪所造成的直接经济损失达 2890 亿元人民币，受害者人均蒙受的直接经济损失约 1200 元人民币。

**数据三：**2012 年仅公安部督办的“2.20”入侵政府网站制贩假证一起案件，就抓获犯罪嫌疑人 165 名，收缴虚假证书 11 万余本、虚假印章 1 万余枚，涉案金额 3 亿多元，被入侵的政府网站多达 185 个，涉及全国除西藏以外的 30 个省区市的人事、财政、卫生、教育、建设、金融等多个部门。

**数据四：**据北京市公安局网安总队负责人介绍，2012 年

北京市公安局共发现处置的各类违法信息 108 万余条，处罚网站 1.7 万余家次，关闭问题突出的栏目 1.9 万余个；破获各类案件 3800 余起，抓获违法犯罪嫌疑人 4200 余名；消除各类网络信息系统安全隐患 1.4 万余个。

上述情况表明，网络违法犯罪形势严峻，坚持依法管网、依法治网，严厉打击各类网络违法犯罪任重道远。

## 一、2012 年中国互联网违法犯罪概况与特点

### （一）2012 年我国网络犯罪总体态势

2012 年我国网络犯罪依然高发，且受害人的规模和涉及金额都十分巨大。赛门铁克公司发布的诺顿安全报告称，2011 年 7 月至 2012 年 7 月，中国估计有超过 2.57 亿人成为网络犯罪受害者，直接经济损失达人民币 2890 亿元。<sup>①</sup>同一时期，被网络犯罪侵害的在线成人达 72%（即每天有超过 70 万名中国网民遭受网络犯罪的侵害，每分钟有 489 名受害者），平均每位网络犯罪受害者蒙受的直接经济损失达到人民币 1126 元。<sup>②</sup>

根据笔者对于媒体报道资料的整理，2012 年我国网络犯罪的主要类型有网络诈骗、网络传销、网络色情、网络钓鱼、网络赌博、网络贩毒、网络贩枪、网络贩卖人体器官、网络

<sup>①</sup>新华网，“网络犯罪致中国年损失 2890 亿元”，[http://news.xinhuanet.com/newmedia/2012-09/13/c\\_123708805.htm](http://news.xinhuanet.com/newmedia/2012-09/13/c_123708805.htm).

<sup>②</sup>中国日报网，“加强网络信息保护”，[http://www.chinadaily.com.cn/hqcj/zxqxb/2012-12-22/content\\_7839482.htm](http://www.chinadaily.com.cn/hqcj/zxqxb/2012-12-22/content_7839482.htm)

非法集资、网络黑客攻击、网络贩卖假药、网络贩卖公民个人信息、网络敲诈勒索、网络传授犯罪方法、网络贩卖爆炸物品、网络贩卖剧毒化学品、网络拐卖人口、利用网络制造传播谣言，散布虚假恐怖信息以及利用网络窃取、泄露国家秘密等。

同时，公安机关也加大了对网络犯罪行为的打击力度，2012年8月，公安部部署全国公安机关开展了深化打击整治网络违法犯罪专项行动。截止10月15日，各地公安机关已查破刑事案件4400余起，抓获犯罪嫌疑人8900余人，清理网上违法有害信息188万余条，集中整治违法有害信息频发、高发的网站3500余家，<sup>①</sup>尤其是侦破了白银“1·17”特大网络传销案、曲靖“5·16”特大网络传销案件、青岛“5·22”特大侵犯网络著作权案、济南“8·02”特大DDOS黑客攻击案、萍乡“9·27”特大网络贩枪案等一系列有重大影响的案件，净化了网络环境。

## （二）2012年我国网络犯罪特点

### 1. 犯罪主体低龄化

纵观2012年的网络犯罪，犯罪主体低龄化的趋势越发明显。例如，在湖北省破获的网络犯罪案件中，犯罪嫌疑人中30岁以下的占90%以上。<sup>②</sup>而在徐州警方破获的网络犯罪

<sup>①</sup>中国广播网，“公安机关打击整治网络违法犯罪 抓嫌犯8900余人”，<http://news.qq.com/a/20121015/001076.htm>.

<sup>②</sup>人民网，“26岁网络‘毒霸’非法获利800万 网络犯罪低龄化明显”，<http://hb.people.com.cn/BIG5/n/2012/1026/c337099-17636972.html>.

案件中，犯罪嫌疑人中 90 后占到了 40%。<sup>①</sup>究其原因，首先是因为现在的黑客攻击技术门槛越来越低，年轻人可以非常方便地获取相关的知识，获取相关的黑客工具；其次是年轻人对于网络的了解和依赖比中年人或者年长者要更深，对于网络上的各种应用与服务也非常熟悉，加上年轻人对于自身行为的后果认识不深刻，所以容易在网络上实施犯罪。

## 2. 网络犯罪产业化，完整的利益链条进一步成形

经过近年的发展，围绕着具体网络犯罪行为，犯罪分子形成了一个完整的利益链条。在链条的每一个环节，犯罪分子分工明确、相互配合，共同完成从准备、组织、物色目标、实施犯罪行为、获取利益、分赃的整个过程。从另一个角度讲，也可以说网络犯罪进行了精细化的分工，而分工结果就是形成内部结构严密的犯罪组织。组织成员依附于整个犯罪链条上，从中获取非法利益，最终形成了与犯罪链条的共生关系。

## 3. 新的犯罪手法不断涌现

随着警方打击力度的加大以及网民防范意识的不断提高，网络犯罪的具体手法也不断推陈出新。例如，目前的网络传销往往要进行精心的设计，并通过“资本运作”、“股权投资”、“电子商务”和“网络销售”等名称进行包装，对不知情的网民进行欺骗，迷惑性非常强。部分犯罪嫌疑人则根

<sup>①</sup>陕西传媒网，“做黑客门槛降低：90 后网络犯罪引关注”，<http://www.sxdaily.com.cn/n/2012/1025/c90-5001250-1.html>

据网络的热点设计新的手法实施犯罪。例如，2012 年 11 月，杭州市公安局和淘宝网联合宣布破获淘宝网首例“恶意差评师”案，经过跨省区联手侦查追捕，7 名犯罪嫌疑人被抓获，并以涉嫌敲诈勒索罪被逮捕。犯罪嫌疑人以给差评为借口向淘宝商家进行勒索，其中一位杨某短时间内作案 40 多次。“差评师”向每家店铺索要的金额通常只有几百元，但作案频率较高，今年 6 月作案高峰期，一天之内就曾攻击 20 多家店铺。<sup>①</sup>网络钓鱼也出现了“潜伏战”、“游击战”两种新的“钓鱼手段”，并且不断根据网络热点选择钓鱼对象。例如，浙江卫视“中国好声音”热播时，部分不法分子便假借节目组的名义制作钓鱼网站骗取用户信息；小米手机热销后，2012 年 5 月、6 月两个月，中国反钓鱼联盟就处理了 56 个仿冒小米手机的钓鱼网站。<sup>②</sup>今年的淘宝双 11 促销日前两天，根据网络安全公司的监测显示，每天新增加钓鱼网站数量就有 3 万个左右。<sup>③</sup>

#### 4. 网络上买卖个人信息的犯罪急剧增加

2012 年 4 月，公安部组织开展了规模空前的打击侵害公民个人信息违法犯罪集中行动，抓获犯罪嫌疑人 1936 名，挖出非法出售公民个人信息的“源头”44 个，破获各类刑事案件 3024 起。此次行动中，长沙警方打掉一个名为“中国

<sup>①</sup> 新华网，“淘宝网首例恶意差评师案告破 打击网络新型犯罪”，<http://sx.sina.com.cn/news/economy/2012-12-03/063934446.html>。

<sup>②</sup> 中国日报网，“‘钓鱼网站’玩潜伏 加强网络立法迫在眉睫”，[http://www.chinadaily.com.cn/micro-reading/dzh/2012-12-21/content\\_7829606.html](http://www.chinadaily.com.cn/micro-reading/dzh/2012-12-21/content_7829606.html)。

<sup>③</sup> 东广新闻台，“网络犯罪直接经济损失达 2890 亿元 个人信息应更受保护”，<http://sh.eastday.com/m/20121224/u1a7082298.html>。



资源部”的信息倒卖团伙。在犯罪嫌疑人的作案电脑中，存储的公民个人信息数据涉及全国几乎所有省份，总量在 1.5 亿条以上，从姓名、电话、住址、房产、车辆到通话详单、航班记录，信息内容门类众多，详细程度令人瞠目。<sup>①</sup>除了银行、电信等部门外，掌握大量个人详细资料的电商也成了信息泄露的重要渠道。上海警方透露，根据网络安全总队的细心排摸调查，已查获“一号店”网上商城与已离职员工及公司外部人员内外勾结，致使 70 万客户信息泄露，警方已控制 11 人。<sup>②</sup>

## 5. 智能手机成为了网络犯罪新阵地

赛门铁克对来自 24 个国家或地区的 13000 多位成年人进行了调查，报告显示新型网络犯罪正转向社交网络或移动设备网络。在过去的一年中，在中国，估计有 43% 的网络成人用户遭受过社交网络或手机网络犯罪的侵害。<sup>③</sup>随着技术的持续发展与成本的不断降低，智能手机普及率持续增加，而其中各种时尚的应用则成为了年轻人的新宠。而犯罪分子也正好利用这点，通过各种应用实施犯罪。<sup>④</sup>

## 二、2012 年中国互联网违法犯罪问题分类分析

### （一）网络诈骗

<sup>①</sup>海南特区报，“网络信息保护路在何方？”，<http://tech.hexun.com/2012-12-23/149366288.html>

<sup>②</sup>赛迪网，“上海警方打击网络犯罪 一号店榜上有名”，<http://roll.sohu.com/20121101/n356392233.shtml>

<sup>③</sup>新闻晚报，“网络犯罪转向社交网络和移动终端”，[http://www.chinadaily.com.cn/micro-reading/dzh/2012-10-15/content\\_7245245.html](http://www.chinadaily.com.cn/micro-reading/dzh/2012-10-15/content_7245245.html)

<sup>④</sup>中国网，“微信成犯罪工具 互联网‘微’时代乱象频仍待整治”，<http://finance.china.com.cn/industry/kj/20120928/1048329.shtml>

## 1. 网络诈骗的概况

网络诈骗是指以非法占有为目的，利用互联网采用虚构事实或者隐瞒真相的方法，骗取数额较大的公私财物的行为。随着网络的普及，一些传统的诈骗手段开始在网络上出现并不断演变、升级，网络的非直接接触式的信息传播和信息交流方式，正好弥补了面对面诈骗时，诈骗分子容易出现的心虚、紧张、面貌容易被识别等缺点，更容易诈骗成功。2012 年网络诈骗方式主要包括网络中奖诈骗、QQ 网络聊天诈骗、网络钓鱼网站或虚假网站诈骗、网络购物诈骗、网络彩票诈骗、网络股票诈骗、网络招聘诈骗、网络高考诈骗等。同时，新型的微信诈骗、网络传销诈骗以及冒充商业合作伙伴网络诈骗不断出现。

2012 年度，钓鱼网站与诈骗网站尤其猖獗。根据中国电子商务协会可信电子商务推进中心、中国可信网站应用推进联盟和可信网站验证管理机构中网（knet.cn）联合发布的《2012 年中国网站可信验证行业发展报告》显示：截止 2012 年 6 月底，31.8% 有网络购物经历的网民本人曾在网购过程中直接碰到钓鱼网站或诈骗网站，网购受骗网民的规模保守估算为 6169 万。超过 39.7% 的网民损失额度超过 500 元。保守估算，每年因钓鱼网站或诈骗网站给网民造成的损失不低于 308 亿<sup>①</sup>。2012 年 1 月 1 日至 11 月 20 日，中国反钓鱼网

<sup>①</sup> 参见中国电子商务协会可信电子商务推进中心、中国可信网站应用推进联盟和可信网站验证管理机构中网（knet.cn）联合发布的《2012 年中国网站可信验证行业发展报告》，来自

站联盟共处理钓鱼网站 24535 个。截至 2012 年 11 月 20 日，联盟累计认定并处理钓鱼网站 100402 个。2012 年钓鱼网站涉及行业前三位，分别为支付交易类、金融证券类、媒体传播类，占处理总量的 94.61%。2012 年联盟接到的钓鱼网站举报中，涉及淘宝网、工商银行、央视、腾讯公司四家单位的钓鱼网站总量占全部举报量的 80.09%<sup>①</sup>。

## 2. 网络诈骗的发展趋势

诈骗，是一种古老的犯罪形式，自古至今一直存在，只是不同时代诈骗手段在不断地发生变化。网络诈骗是借用了网络平台来实施的诈骗行为，随着网络的逐渐普及，网络诈骗在将来仍然会持续存在。

全国人大常委会于 2012 年 12 月 28 日颁布的《关于加强网络信息保护的决定》第六条规定：网络服务提供者为用户办理网站接入服务，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服务，应当在与用户签订协议或者确认提供服务时，要求用户提供真实身份信息。本条规定明确地要求提供网上信息者的身份必须真实，从而有利于打击利用虚假身份提供虚假信息来实施网络诈骗的行为。

网络社会是虚拟的，但它又高度对应现实社会，虚实两个社会的高效互动造成了互联网影响力的几何性扩大，逐渐

---

[http://ectrust.knet.cn/column\\_2/201207/t20120704\\_30604.html](http://ectrust.knet.cn/column_2/201207/t20120704_30604.html)。

<sup>①</sup> 参见中国反钓鱼网站联盟颁布的《2012 年中国反钓鱼网站联盟年报》，资料来源：<http://www.apac.org.cn/>。

成为中国各种信息和意见集散、流动的中枢<sup>①</sup>。同样，网络诈骗与现实社会的诈骗所具备的土壤仍然存在，网络诈骗与现实社会的诈骗又是互动的，互联网只是加剧了诈骗的范围、诈骗的隐蔽性、诈骗的多样性，但万变不离其宗，本质上仍然是编造虚假信息或隐瞒真相骗取他人财物的行为。尽管《关于加强网络信息保护的決定》明确规定了提供信息者要使用真实身份，但是，借鉴现实社会中的诈骗案例，试问：谁来有效监督网站服务者是否真正实施了身份的核实？如何确保提供的身份信息的真实性？如何保证提供的身份信息就是上网者本人的真实信息呢？网上所提供的信息的真实性谁来核实？对于在境内可以上的境外网站发布的信息谁来监督？等等。

所以，《关于加强网络信息保护的決定》的颁布，会增强网络诈骗实施的难度，有效控制网络诈骗的发生，但不会也不可能杜绝网络诈骗的发生。实际上，对照现实中的诈骗行为，网络诈骗的存在的氛围仍然继续存在，如网站的真实性、个人身份的真实性、网上信息的真实性等都难以确保完全准确。缺乏有效的监督，就难以遏制虚假信息的传播，难以及时发现虚假网站的存在。由此可见，未来网络诈骗的数量仍然会处于一个高位运行的状态，网络中奖诈骗、网络购物诈骗、网络钓鱼诈骗、网络传销诈骗仍将比较突出。

---

<sup>①</sup> 社评：加强互联网管理是得人心的，载《环球时报》2012年12月21日。

### 3. 网络诈骗的特点

网络诈骗主要是利用了互联网迅速的传播速度和广泛的传播范围进行的违法犯罪行为，与传统的诈骗行为本质上是一样的，就是编造虚假信息或隐瞒真相，骗取对方财物的行为。网络诈骗主要具有以下几个特点：

#### （1）犯罪手段复杂性

网络诈骗手段复杂多变，除了传统的购物诈骗、征婚诈骗外，现在的视频聊天诈骗、中奖诈骗、钓鱼网站诈骗、微信诈骗等手段层出不穷。一方面，一些网络诈骗手段在网络上不断传播，一些人逐渐加入网络诈骗的队伍行列；另一方面，网络诈骗分子不断总结诈骗技巧，不断演练诈骗场景，不断完善诈骗手段，使得网络诈骗不断演变、不断升级，手段更加复杂多变。

#### （2）隐蔽性

网络诈骗行为人使用虚假身份在网络上发布虚假信息或创建虚假网站，骗局设计得极具诱惑性，紧紧抓住受害人的心理，使得受害人“自愿”交出钱物。如在中奖、折扣、低价等骗局中利用的是人们“贪小便宜”的心理；在视频聊天诈骗中利用人们的亲友信任的心理。从形式上看，这些网络诈骗合乎常理，隐蔽性强，容易使人上当受骗。

#### （3）跨区域性

网络的触角可以延伸到任何能够上网的角落。同样，诈骗信息也会传播到全国甚至世界各地。大部分这类案件是跨地区、跨省甚至跨国境的犯罪行为。这也为警方及时、有效地打击带来了难度。

#### （4）非接触性

传统的诈骗手段基本上都是面对面的诱惑，使用语言或者其他手段作为道具进行当面诈骗钱财。但是网络诈骗案件中，一般是诈骗行为人在网络上发布虚假信息，诱使受害人出于贪利、信任、警惕性不高等原因，受诈骗信息诱导，一步步进入已经设好的骗局，上当受骗。在整个受骗过程中，受害人与诈骗行为人一般没有直接面对面的接触，只是通过网络进行信息的沟通和交流。

#### 典型案例：

2012年6月，福建省福州市公安局网安部门侦查发现，网民“神鹰黑客联盟”、“火影黑客联盟”等在各大网站论坛大量发布非法广告，自称能利用黑客手段获取公民个人隐私信息，可承接各种密码破解、银行卡查询、即时通讯破解、IP查询、手机话单查询、手机定位、手机监听等业务。经查，这是一起以“黑客联盟”为幌子实施诈骗的新型犯罪案件，犯罪嫌疑人利用受害者因抱有非法获取他人个人隐私资料的不正当目的，即使受骗也不敢向公安机关报案的心理，疯狂实施网络诈骗，受害者涉及全国各省市4000多人，涉

案金额达上百万元。2012 年 7 月 24 日，公安机关成功抓获苏某某等 3 名犯罪嫌疑人<sup>①</sup>。

## （二）网络色情：概况、趋势、特点与典型案例

所谓色情，一般是指以引起性兴奋为目的，而展示或描述人类身体或人类性行为的一种表现。色情存在的媒介包括文字、照片、雕像、绘画、音频、视频、动画等。网络色情则是指利用国际互联网进行传播的具有上述内容和形式的色情媒介。

### 1. 当前我国网络色情发展概况

网络色情是伴随网络发展而来的，长期以来，我国有关部门一直坚持对网络色情的严厉打击，特别是经过 2009 年初开展的“七部委联合整治互联网低俗之风”、2009 年底和 2012 年 3 月至 8 月开展的“九部门深入开展整治互联网和手机传播淫秽色情及低俗信息”专项行动，以及于 2010 年 12 月召开整治互联网和手机淫秽色情信息现场经验交流会以来，各地区、各相关部门持续开展了整治打击网络色情的一系列专项治理行动，网络色情蔓延之风得到了一定程度的遏制。但是，由于互联网技术与应用的发展，一些网站传播网络色情的问题又有所抬头，网络色情和低俗信息传播形式和渠道更加复杂多样；网络色情传播的问题并未得到有效遏制，网络色情传播案件包括利用网络传播淫秽物品行为与传

<sup>①</sup> 李恩树 卢杰：公安部公布一批网络违法犯罪典型案例，载人民网 2012 年 12 月 28 日，网址：<http://legal.people.com.cn/n/2012/1228/c42510-20040294.html>。



播淫秽物品牟利行为均还比较多发；网络色情传播的形式也日益多样化，利用论坛型色情网站、交友型色情网站、线上色情视频聊天平台（包括视频网站、网上即时通讯工具）等传播网络色情问题依然突出；网络色情涉及的社会面和社会群体有进一步扩散之势。

## 2. 当前我国网络色情的主要特点

（1）网络色情形式日益多样化。随着互联网技术的发展和网络应用的日益多样化，这些网络技术和应用在给人们带来极大便利的同时，也带来了网络色情传播形式的多样化。除传统的论坛型色情网站如论坛、贴吧、博客、微博客，社交（交友）型色情网站，搜索引擎网站、音视频网站外，还包括即时通信群组即网上即时通讯工具如 qq 群组及个人 qq 工具，手机网站，网络游戏网站等，以及利用移动智能终端应用程序平台、在线视频播放软件、网络共享网站（服务器）、网络资源下载工具等网络新应用传播网络色情等。

（2）网络色情传播者牟利目的与非牟利目的共存。一般而言，传统的网络色情的传播者都是以牟利为目的的，其传播网络色情的动机主要在于谋取个人私利而不顾及负面社会影响与法律的制裁，从而构成传播淫秽物品牟利罪。如 2012 年 11 月，江苏省新沂市人民法院宣判了该院首例传播淫秽物品牟利案，被告人陈某被判处有期徒刑三年，并处罚金人民币 5000 元。2011 年 5 月，犯罪嫌疑人陈某为了赚钱，



萌生了开设色情网站的念头，建立了自己的网站，成为该网站的管理员，并利用网站上的淫秽信息吸引网民进入其网站点击和浏览，通过收取VIP会员注册费的方式进行牟利，且会员通过发帖当上管理员后就享有免费观看色情图片、视频、小说等虚拟的权力，同时，以网民的点击率吸引广告商在该网站投放广告以牟取广告费。

与传播淫秽物品牟利不同，网络色情传播的另一种动机则是不以牟利为目的，其传播的动机主要是通过网络色情传播行为（与他人共享）提高自身的浏览权限。如在政府部门工作的田某出于获取积分，从而赢得更大的网站浏览权限的动机，在办公室内利用个人笔记本电脑，往色情网站上传多部淫秽文章，以达到浏览更多淫秽视频、文章和图片的目的，从而构成了传播淫秽物品罪。

（3）网络色情传播途径日益多样化、移动化。随着移动互联网和平板电脑与智能手机等多种移动网络终端设备的发展，人们的上网工具和上网途径日益多样化、移动化。除传统的上网终端电脑和笔记本外，平板电脑与智能手机等便携式移动上网终端也逐渐成为网民上网、网络色情传播的重要终端和途径之一，尤其是对于高学历、低龄化的网民群体而言更为突出；同时，由于移动互联网发展具有的移动性与低约束性，大大提高了网络色情信息的可获得性，导致网络色情信息的传播更为便利。如2012年中国青年网、中国青

少年网络协会和中国传媒大学调查统计研究所联合发布的《未成年网民网络色情信息接触状况研究报告》显示：“未成年人在使用不同上网设备遭遇网络色情信息的选择中，比例最高的是电脑，为 61.7%，其次是平板电脑，为 37.9%，再次是手机，为 19.6%。”

（4）网络色情传播行为打击难度大。与传统色情网站通过会员制收取费用获利、打击相对较为容易相比，近来出现的色情网站往往对网民而言是免费的，色情网站通过广告联盟（一种介于色情网站与广告主之间的广告中间商）按网站流量经由第三方支付平台获取广告费，网站服务器系租用境外服务器且不断变换网站地址以逃避打击，从而加大了打击的难度。如 2012 年，由公安部督办的江苏扬州“2·03”双倍广告联盟传播淫秽物品牟利案，计算机专业毕业的犯罪嫌疑人色情网站站长李某，通过从网上租用服务器，花钱购买 IP 地址，从别的网站上移植色情内容，建立色情网站。与传统淫秽网站收取会员注册费的盈利模式不同，该网站通过加盟广告联盟，获取开放广告代码，在自建的淫秽网站上投放广告联盟所提供的成人用品、医疗保健品、药品等低俗广告，通过访问其淫秽网站网民的点击数获取非法广告费，并通过第三方支付平台进行支付，从而形成广告主、色情网站、广告联盟、第三方支付平台的隐蔽性非法利益链条。

### 3. 当前我国网络色情发展的新趋势

(1) 网络色情的传播者进一步低龄化、高学历化。由于互联网发展与应用客观上需要以计算机网络知识为基础，这就为具有高学历特别是具有计算机专业背景的年轻人提供了机遇，一些高学历的年轻人在利益的诱惑下走上利用色情网络犯罪的道路也就不足为奇了。同时从网络色情的受众角度看，高学历、低龄化人群也是网络色情信息的主要接受者和传播者。网络色情传播者进一步低龄化、高学历化成为一种必然趋势。

(2) 网络色情传播的非牟利化趋势进一步显现。与网络色情的传统传播者不同，随着越来越多的高学历年轻群体接触网络成为网民，其成为网络色情的传播者，动因并不在于牟取非法利益，而是由其工作性质、生活方式与社会思潮等共同影响而形成的一种所谓“个体需求”。无论这种需求出于何种动机，客观上都导致了非牟利化的网络色情传播进一步显现出与传统网络色情传播者的迥异之处，这也预示着网络色情的治理将是一个长期、复杂而艰巨的任务，需要从社会治理的层面多角度多渠道地应对这一问题。

### **(三) 网络赌博：概况、趋势、特点与典型案例**

#### **1. 网络赌博概况**

##### **(1) 定义**

赌博<sup>①</sup>：是一种拿有价值的东西做注码来赌输赢的游戏，

---

<sup>①</sup> 该定义来自维基百科

是人类的一种娱乐方式。任何赌博在不同的文化和历史背景有不同的意义。目前，在西方社会中，它有一个经济的定义，是指“对一个事件与不确定的结果，下注钱或具物质价值的东西，其主要目的为赢取更多的金钱或物质价值”。通常情况下，下注的结果，可以在短时间内看到。

网络赌博<sup>①</sup>：通常指利用互联网进行的赌博行为。网络赌博种类繁多，基本上现实生活中主要的赌博方式在网络中都可以进行，主要包括：以六合彩为代表的私彩赌博，通过互联网接受私彩投注，目前主要是依托香港六合彩而由个人组织的外围网上投注；以赌球为代表的体育竞技类赌博，以体育比赛特别是足球赛作为赌注对象，通过网上投注进行赌博活动；以百家乐为代表的境外赌场网络视频赌博，通过网络视频观看境外赌场实况并委托代理人下注，其中“百家乐”、“龙虎斗”是网络视频赌博最常见玩法。

## （2）分类

网络赌博主要分为两大类，一类是传统的赌博转移到网络上，利用网络互动性强、隐蔽性强、支付方便、证据保全等特点开展赌博活动，由于网络的即时性和跨区域性更有可能大大增加参赌的范围，从而使网络赌博的数额不断升级，前不久辽宁就审理了一起涉案金额达 58 亿元人民币的网络赌博案件。另一类是网络游戏中衍生的一些赌博活动，

---

<sup>①</sup> 该定义摘录央视网

即“变相的赌博类网络游戏”，涉及网络游戏服务、虚拟货币、第三方交易平台等多个环节，采取一些打法律“擦边球”的形式，赌资往往不直接与人民币挂钩。与前一类赌博形式相比，在界定上有一定的困难。而这种网络赌博形式一旦发展起来，由于其相当的隐蔽性和我国目前庞大的网络游戏用户的存在，其传播范围可能更广、发展变化更快。

### （3）特点

在许多经济发达地区，参与网络赌博的资金、人数已经超过“实体”的地下赌场，成为众多赌徒的第一选择。网络赌博多采用最简单的押大小方式，貌似输赢机率五五开，但由于以虚拟界面代替了面对面的博弈，这种不透明的方式使得骗术层出不穷。网络赌博有没有赢家？有，但只有设局者获利。

另外，网游赌博平台日益国际化、玩家分散性强，数量大、网游赌博人群年轻化，越来越多青少年参与到网游赌博之中、专业化网络赌博公司越来越多，组织结构更加严密、网络便捷使赌资支付渠道网络化，电子化程度更高、赌资数额巨大，赌资运转速度加快。

### （4）趋势

据了解，2010年6月13日，公安部公布打击网络赌博犯罪十大案例，其中三例为广东侦破，珠海“国际会”、深圳“克拉克”等网络赌博案均名列其中。据广东警方介绍，

目前的网络赌博专业分工强，网站运作、推广、赌金支付等均有各环节承担。这为打击赌博增设了难度。同时，广东警方表示，在现有形势下，相关法律明显滞后，对网络赌博量刑和电子取证等需有进一步明确，以此加强打击力度<sup>①</sup>。

据介绍，在网络赌博中，赌球是主要方式。此外，警方在办案中发现，一些涉赌人员利用一款“打水软件”在足球赌博网络上投注，该软件通过对不同赌博网站提供的赔率差进行测算，在不同网站同时下注，从而赚取利润差以及网站给代理者的返点。办案民警表示，这种软件是最新出现的一款技术软件，代表了网络赌博的一个新趋势。

### （5）危害

近来网络赌博非常活跃，不少迷恋上网络赌博的人，倾家荡产，妻离子散。另外，网络赌博不需要进行现金交易，为洗钱犯罪提供了便利条件，有数据显示，境外网络赌博每年从我国抽走上千亿资金，造成我国资金严重外流。

## 2. 典型案例分析

### 广东深圳“10·09”特大网络赌博案

2010年4月中旬，广东省深圳市公安机关发现，服务器托管于香港的新型实时在线视频赌博网站“克拉克网上娱乐场”和“东城娱乐场”以龙虎斗、百家乐、二八杠、轮盘、骰宝等赌博游戏的方式，吸引中国境内会员进行网上参赌，

---

<sup>①</sup> 该部分摘录自南方日报

已发展会员 6000 余名。这两个赌博网站属于同一个赌博集团所控制，该赌博集团成员大多活动于深圳和菲律宾等地，并通过“境内外勾结—依托境外赌场—外置人员和机构—组织网上赌博”的营销模式逃避公安机关打击。经近一个月的缜密调查，5 月 18 日，广东深圳公安机关成功侦破该案，一举抓获包括该赌博集团首脑周某某在内的主要成员 5 人，冻结银行资金 1500 余万，现场查扣银行卡近 50 张，宝马 X5 越野车一部、电脑 4 台，手机 8 部。

分析：近几年，一种“非代理制”的网络赌博开始出现。由于其采用更为简便的方式入会，发展会员的速度异常迅猛。2010 年 5 月 18 日，深圳警方破获的“克拉克网上娱乐城”视频赌博，采取的就是“非代理制”运营方式。而且“克拉克”还采取了一种有别于传统网络赌博的新赌博方式“真人棋牌”。“真人棋牌”是从真实赌场传来的同步视频，可以看见赌场荷观（发牌员）在现场发牌，会员通过网银购买网络筹码后，便可以与场内的赌客一样下注，片刻见输赢，身临其境，作为一种新的网络赌博形式，这也叫“真人荷观”、“真人荷手”。打开“克拉克”网页，载有宣传娱乐场的广告，还有国内 400 开头的免费电话，电话打通后就被转接到菲律宾的客服人员处，客服人员全由大陆派往菲律宾。网站采取的运营方式就是“非代理制”，不经过层层招募代理人，会员直接与赌场发生关系，每个加入的会员都会得到一个虚拟账户，

会员向赌场提供的银行账号存钱后,虚拟账户内就有相应的赌博筹码,筹码也可以变现。“采取这种在线非代理制方式发展会员,更加便捷。”深圳市网警支队三大队大队长左明春介绍,“克拉克”自2009年3月运营到2010年5月被摧毁,就已发展会员6000多人。

### (3) 法律惩罚

中国《刑法》第303条规定了赌博罪,该条规定:以营利为目的,聚众赌博、开设赌场或者以赌博为业的,处三年以下有期徒刑、拘役或者管制,并处罚金。

据公安部网站消息,日前,最高人民法院、最高人民检察院、公安部联合出台《关于办理网络赌博犯罪案件适用法律若干问题的意见》,针对利用互联网、移动通讯终端等传输赌博视频、数据,组织网络赌博等犯罪行为,进一步明确了法律适用标准。《意见》规定了利用互联网、移动通讯终端组织网络赌博活动,构成开设赌场罪的定罪量刑标准。另外,还规定了明知是赌博网站,而为其提供互联网接入、服务器托管、网络存储空间、通讯传输通道、投放广告、发展会员、软件开发、技术支持、资金支付结算等服务或者帮助,以开设赌场罪的共同犯罪处罚的定罪量刑标准等。据介绍,最高人民法院、最高人民检察院、公安部出台该意见,是为了进一步打击网络赌博犯罪,切断相关利益链条,解决办理



该类刑事案件所面临的法律适用疑难问题。

#### **（四）制作、复制、传播有害信息**

##### **（1）网上制作、复制、传播有害信息的概念与犯罪类型**

###### **①概念**

公安部《计算机信息网络互联网安全保护管理办法》（以下简称《办法》）第四条规定，任何单位和个人不得利用互联网危害国家安全泄露国家秘密，不得侵犯国家的、社会的、集体的利益和公民的合法权益，不得从事违法犯罪活动；第五条规定，任何单位和个人不得利用国际联网制作、复制、查阅和传播公然侮辱他人或者捏造事实诽谤他人的信息。

《中华人民共和国电信条例》（以下简称《电信条例》）第五十七条对网上制作、复制、传播有害信息的内容作了规定，即：任何组织或者个人不得利用电信网络制作、复制、发布、传播含有下列内容的信息：（一）反对宪法所确定的基本原则的；（二）危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；（三）损害国家荣誉和利益的；（四）煽动民族仇恨、民族歧视，破坏民族团结的；（五）破坏国家宗教政策，宣扬邪教和封建迷信的；（六）散布谣言，扰乱社会秩序，破坏社会稳定的；（七）散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；（八）侮辱或者诽谤他人，侵害他人合法权益的；（九）含有法律、行政法规禁止的其他内容的。

## ②主要犯罪类型

通过制造、复制、传播有害信息而形成的犯罪行为包括：

①煽动分裂国家、破坏国家统一罪；②煽动颠覆国家政权、推翻社会主义制度罪；③煽动民族仇恨、民族歧视罪；④煽动群众暴力抗拒国家法律、行政法规实施罪；⑤利用计算机实施制作、复制、出版、贩卖、传播淫秽物品牟利罪；⑥编造并且传播影响证券交易的虚假信息，扰乱证券交易市场罪；⑦虚假广告罪；⑧捏造并散布虚伪事实，损害他人的商业信誉、商品声誉罪；⑨传授犯罪方法罪；⑩侮辱、诽谤罪等

## (2) 网上制作、复制、传播有害信息的现实危害

### ①引发社会恐慌

有可能会产生一些无法预知、无法挽回的后果。比如2011年上半年网上出现的加碘盐可以防核辐射的谣言，就导致了多个城市的抢购潮，虽然谣言很快被平息，但是造成社会上人心惶惶、市场秩序一度混乱。

### ②影响国家、政府形象

2012年有人曾在网络传播“军车进京”、“北京夜里响起了枪声”。但实际上这是子虚乌有的凭空捏造，相关责任人已被处罚。这类谣言极易造成群众的恐慌心理，对政府形象造成极坏的影响。

### ③有悖社会道德风尚

有害信息的传播，大到泄露国家机密、损害国家荣誉利益、破坏民族团结、宣扬邪教和封建迷信，小到散布淫秽暴力信息、侮辱诽谤他人，都与中华民族“忠孝诚信、礼义廉耻”的基本道德风尚相违背。

### (3) 网上制作、复制、传播有害信息的法律规制

解决有害信息在网络上的制造、传播等问题，首先需要公民的责任意识。不管是舆论的发起者还是网站的管理者，甚至围观的网民朋友们，都应该树立责任意识，各自在自己的责任范围内维护好网络秩序，不能让有害信息肆意传播，甚至危害大多数人。但是法律的规制也必不可少，在网上制作、复制、传播有害信息的，要按照《电信条例》、《刑法》、《治安处罚法》和《计算机信息网络国际联网安全保护管理办法》进行处理，除承担民事责任、行政责任外，情节严重的还要追究刑事责任。

《电信条例》第七十八条：有本条例第五十七条、第五十八条和第五十九条所列禁止行为之一，情节严重的，由原发证机关吊销电信业务经营许可证。

《电信条例》第二十条 违反法律、行政法规，有本办法第五条、第六条所列行为之一的，由公安机关给予警告，有违法所得的，没收违法所得，对个人可以并处五千元以下的罚款，对单位可以并处一万五千元以下的罚款；情节严重的，并可以给予六个月以内停止联网、停机整顿的处罚，必要时

可以建议原发证、审批机构吊销经营许可证或者取消联网资格；构成违反治安管理行为的，依照治安管理处罚条例的规定处罚；构成犯罪的，依法追究刑事责任。

例如在网上侮辱、诽谤他人的行为，首先应承担行政责任。按照《办法》第二十条的规定，对网上骂人者，将由公安机关给予警告，有违法所得的，没收违法所得，对个人可以并处五千元以下的罚款；构成违反治安管理行为的，依照《治安管理处罚条例》的规定处罚。

其次应承担民事责任。民法通则第一百二十条规定：公民的名誉权受法律保护，网上对他人进行侮辱、诽谤，实际上仍然属于一般侵权行为，只不过侵权的方式和载体比较特殊而已。由于网络的高度开放性及网上言论的随意性，对社会的巨大影响不可低估，在网上辱骂他人，对他人名誉带来的损害有时比日常生活中辱骂他人更加严重。所以利用互联网辱骂他人，应依法承担民事责任。

第三，如果网上公然侮辱他人，情节严重的，还可能构成侮辱罪而承担刑事责任。按照我国刑法有关规定，侮辱罪是指以暴力或者其他方法，公然贬低他人人格，毁坏他人名誉，情节严重的行为。就网络上骂人传播的速度、范围以及影响力来看，应该认定为“公然”。刑法规定：公然侮辱他人或者捏造事实诽谤他人，情节严重的，处三年以下有期徒刑、拘役、管制或者剥夺政治权利。

如果发现有网民利用国际联网制作、复制、查阅和传播公然侮辱他人或者捏造事实诽谤他人的信息。可按照公安部发布的《计算机信息网络国际互联网安全保护管理办法》的有关规定，保留有关原始记录，并在二十四小时内向当地公安机关报告。

另外对于利用计算机实施制作、复制、出版、贩卖、传播淫秽物品牟利罪，刑法上也有相关规定：

《刑法》第 363 条第一款的规定，以牟利为目的，制作、复制、出版、贩卖、传播淫秽物品的，处三年以下有期徒刑、拘役或者管制，并处罚金；情节严重的，处三年以上十年以下有期徒刑，并处罚金；情节特别严重的，处十年以上有期徒刑或者无期徒刑，并处罚金或者没收财产。

《刑法》第 364 条规定，传播淫秽的书刊、影片、音像、图片或者其他淫秽物品，情节严重的，处二年以下有期徒刑、拘役或者管制。组织播放淫秽的电影、录像等音像制品的，处三年以下有期徒刑、拘役或者管制，并处罚金；情节严重的，处三年以上十年以下有期徒刑，并处罚金。制作、复制淫秽的电影、录像等音像制品组织播放的，依照第二款的规定从重处罚。向不满十八周岁的未成年人传播淫秽物品的，从重处罚。

#### ① 民事责任案例

2012 年，顺德一男子在女友提出分手后，男方怀恨在心，不仅多次电话骚扰前女友，而且在自己的 QQ 空间等网络上发表侮辱诽谤前女友的文章，导致前女友在原单位承受不住压力而失业。经过审理，法院认为，鉴于网络世界维权的特殊性，决定应由发帖者进行举证，最后判处该男子停止侵权，同时向前女友公开道歉与赔付精神损害抚慰金。

## ② 治安行政处罚案例

2012 年，网民“帕米尔-亚森”通过家中电脑登陆境外网站，看到有关“库尔勒市发生一起学经儿童死亡事件”的歪曲报道，在未做任何调查、核准事实的情况下，于 2012 年 5 月 28 日 7 时 05 分，通过新浪微博发布“维（吾尔）少年学习古兰经被扣在拘留所离奇死亡”等信息后，其又多次转发、散布虚假有害信息和言论。网民“帕米尔-亚森”所发信息系境外敌对势力恶意捏造歪曲事实、混淆视听。乌鲁木齐公安机关经过查证，认为网民“帕米尔-亚森”通过新浪微博散布捏造歪曲事实的信息和带有煽动性的言论，扰乱社会秩序，造成社会危害。其行为违反了《中华人民共和国治安管理处罚法》第四十七条的规定。公安机关依法对其处以十五日行政拘留。<sup>①</sup>

2010 年 5 月，上海网民范某出于对其所在公司行业规定的不满，在互联网某论坛中发表言论，煽动该行业员工罢工。

<sup>①</sup>新疆网民微博恶意散布虚假信息 被行政拘留 15 日.[EB\OB].(2012-6-4).法制网  
[http://www.legaldaily.com.cn/legal\\_case/content/2012-06/04/content\\_3616926.htm?node=33809](http://www.legaldaily.com.cn/legal_case/content/2012-06/04/content_3616926.htm?node=33809)

经警方调查，范某的行为已经触犯了《计算机信息网络国际联网安全保护管理办法》，依照相关法律规定，警方对其处以行政警告并处五百元罚款。

2010年2月，上海互联网多个网站上出现了攻击政府机关的图片发帖，此帖引发警方高度重视。经查证，网民朱某为泄私愤，利用自己拍摄的照片和网上下载的图片，采用恶意拼接、剪辑的方法捏造了上述图片并在互联网上广为发布，误导网民。朱某的行为触犯了《治安管理处罚法》，其被警方依法予以治安处罚。

### ③刑事处罚案例

2012年6日下午3时许，网民“避孕要从娃娃抓起”在国内知名网络论坛天涯社区发帖子称“佛山一栋在建的16层高楼坍塌”，并配发一张建筑工地疑似冒烟尘的照片，酷似建筑物倒塌场景。大约1小时之后，新浪微博认证为“天涯杂谈首席版主”的@周丕东在微博中转发了该帖子。这条微博立即引起网民尤其是佛山市民的极大关切。在不到一个小时的时间内，该微博被转发2000多条，评论达到500条。该帖子还在全国各大论坛上广为传播。10日上午，广东佛山公安在湖北省武汉市将在网上故意谣传“佛山在建高楼坍塌”的男子赵某(男，23岁，湖北省枝江市人)抓获。当晚，

警方将其带到佛山，以涉嫌编造虚假恐怖信息罪将赵某刑事拘留。<sup>①</sup>

## （五）破坏网络系统安全

### 1. 概况

2012 年，我国基础网络运行总体平稳，未发生较大规模网络安全事件。根据国家互联网应急中心（CNCERT）公布的 1 月至 11 月数据：国家信息安全漏洞共享平台（CNVD）收集整理信息系统安全漏洞 6285 个，我国境内感染网络病毒的终端数 5417 万台，被篡改网站数量 26471 个，针对境内网站的仿冒页面 27030 个，中国互联网协会反垃圾邮件中心接受垃圾邮件举报 77438 起，CNCERT 接收到网络安全事件报告 17927 起。总体上，公共互联网网络安全态势继续保持平稳运行。

### （1）网络安全目标

网络安全目标主要是保持数据的机密性、完整性、可用性、真实性和可控性。机密性指的是当数据传递时，除了被授权的人，不会受到外力的截取。完整性指的是当数据送达时必须保证数据没有被篡改。可用性是指所有的系统和信息资源必须能够按照机构的需求启动和运行。真实性指的是当传送方提交信息时，就必须能确认传送者的身份是否为冒名。可控性是指对网络信息的传播及内容具有控制能力的特

<sup>①</sup> 23 岁男子网上谣传广东在建高楼坍塌被刑拘  
[EB/OL].[2012-10-11].<http://www.chinanews.com/fz/2012/10-11/4239297.shtml>.



性。

## （2）网络攻击动机

互联网正改变着世界，塑造着新的政治、经济、文化、社会和军事形态，酝酿着新的文明冲突和国际政治关系。国家，组织和个人之间的冲突在网络世界中发挥了关键作用。为了控制全球互联网，推行网络霸权，某些国家在互联网上“攻城略地”；为引起政府和社会的注意，“黑客行动主义者”可能会在网站的主页上留下醒目的留言，引起网络拥塞，或者在网页中嵌入某些激烈的反对观点。甚至可能在网站上加载“拒绝服务攻击”来造成站点瘫痪。出现更多政府资助的网络攻击；为了获取所需情报，网络间谍一般非法入侵敌方或国外计算机网络，截取敌方或国外计算机网络信息，收集整理敌方或国外计算机网络上的公开信息等；为获取高额利润和探寻各种秘密，运用计算机技术，借助于网络对其系统或信息进行破坏或利用。

对于包括利用黑客攻击盗窃网络银行账号、游戏装备；利用黑客手段敲诈勒索或恶性竞争；攻击政府、金融、交通、电力、教育、科研等各个领域的公共服务信息系统。绝大多数黑客攻击以牟利为目的，社会危害性越来越大。此外，制作、出售黑客工具及教授黑客攻击技术已形成地下产业链。

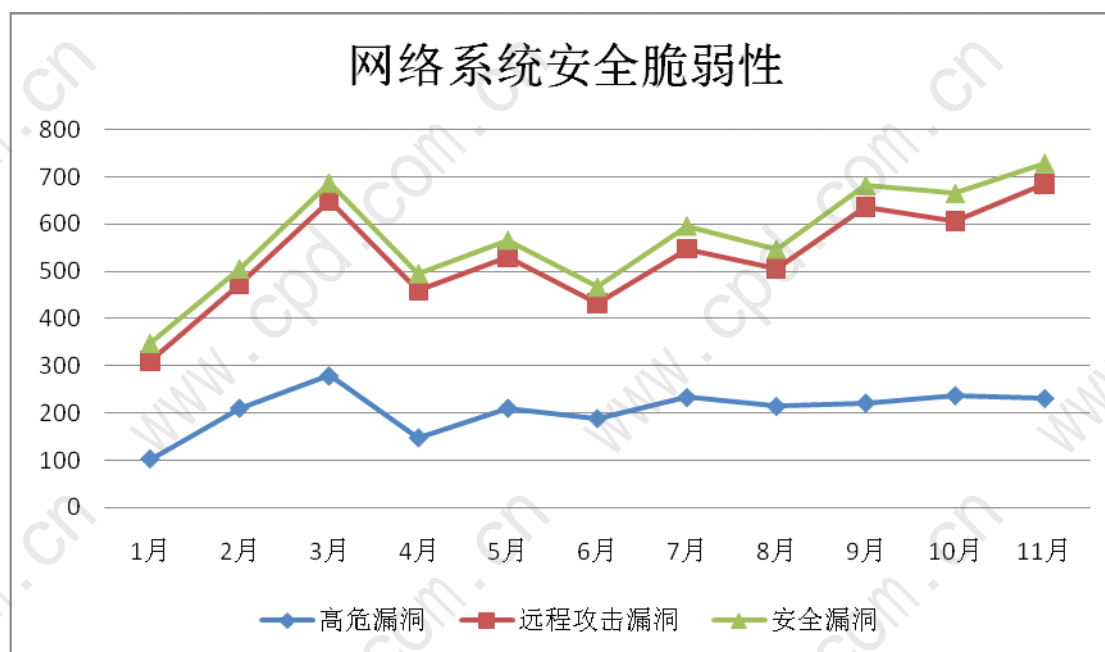
2012年影响较大的黑客攻击破坏案件有“浮云木马”网银盗窃案、攻击敲诈香港金融业网站案、广东揭阳“2·20”非法入侵

计算机系统案等。

## 2. 公共网络环境安全形势

### (1) 安全漏洞

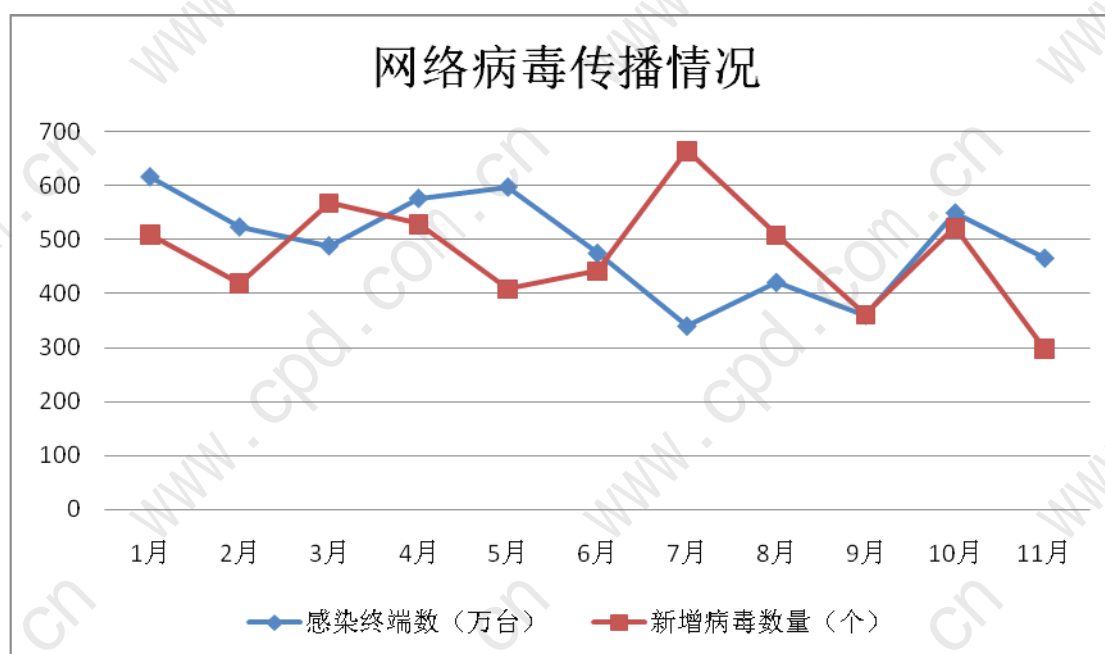
安全漏洞是指网站中的软件、硬件或通信协议中存在缺陷或弱点，从而可使攻击者在未授权的情况下访问或破坏系统，导致信息系统面临安全风险。不同的网站漏洞的危害程度也各不相同。在最坏的情况下，攻击者可以利用此类漏洞完全控制整个网站，甚至绕过系统底层的防火墙控制整个服务器。2012 年 1 月至 11 月，CNVD 收集整理信息系统安全漏洞如下图所示。



### (2) 网络病毒

网络病毒包括木马、僵尸、蠕虫等恶意程序。病毒能自行复制，或者篡改应用软件或系统的可运行组件，或是删除

文件、更改数据、拒绝提供服务，常借助电子邮件、文件档案的宏指令或者可执行文件来散布，影响信息系统正常运行，病毒通常具有一定的潜伏期。特洛伊木马（简称木马）是以盗取用户个人信息，甚至是远程控制用户计算机为主要目的恶意代码。僵尸程序是用于构建大规模攻击平台的恶意代码。蠕虫是指能自我复制和广泛传播，以占用系统和网络资源为主要目的恶意代码。2012 年 1 月至 11 月，CNCERT 监测的网络病毒传播情况如下图所示。

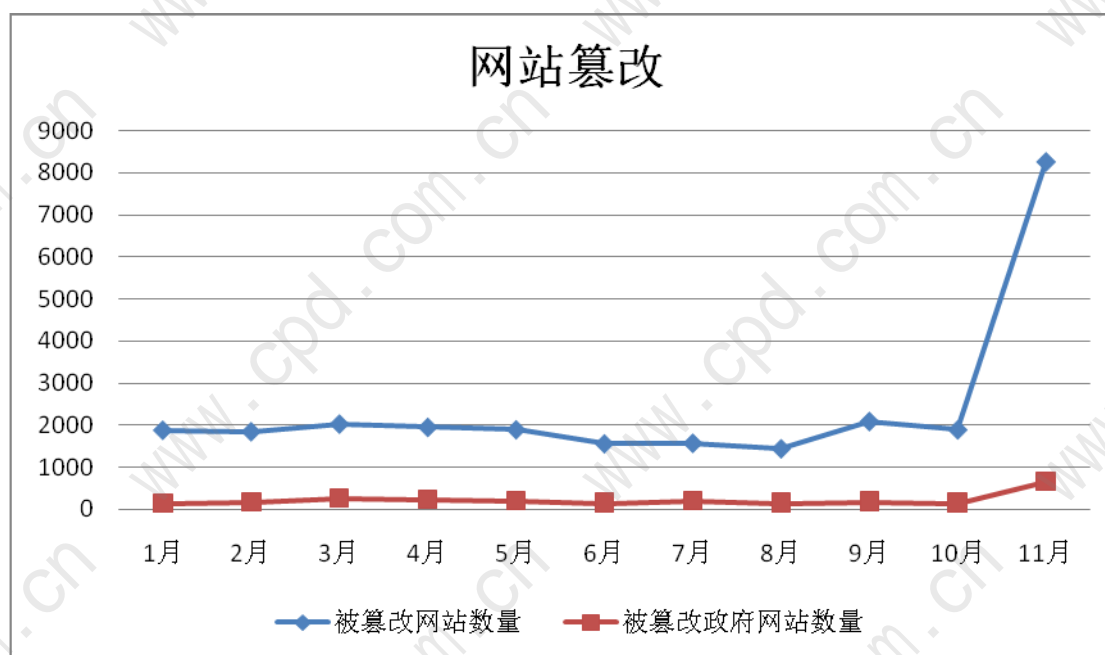


### （3）网站安全

破坏网站安全的行为主要包括篡改、仿冒网页，在网页中嵌入恶意代码（木马），控制网站后门等。

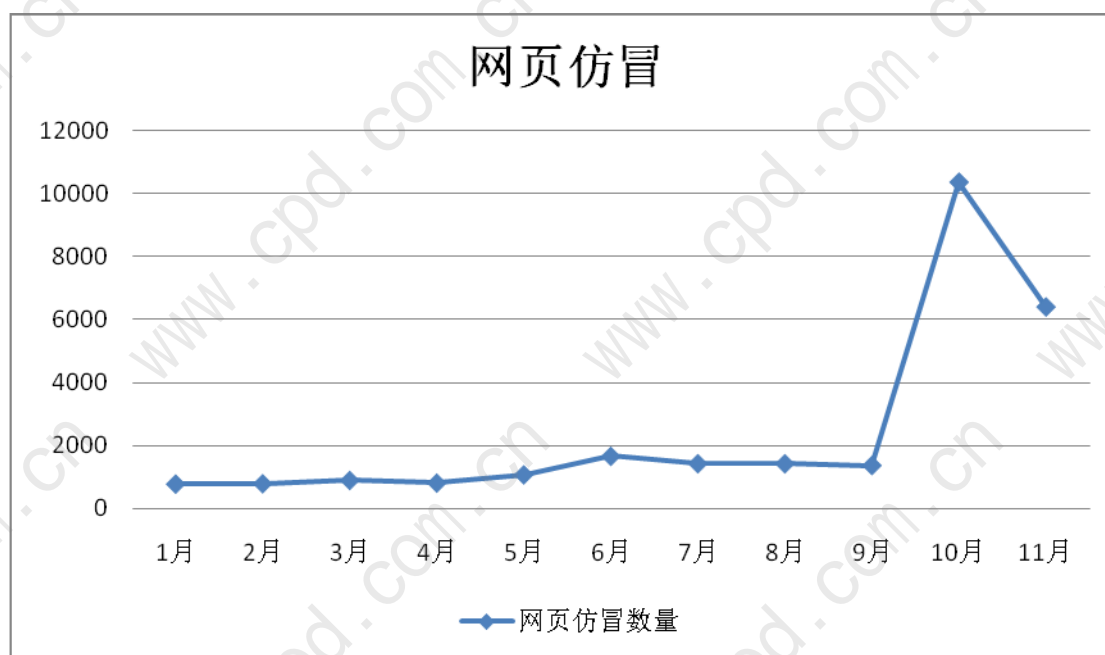
#### ①网页篡改

网页篡改是指攻击者在获取网站控制权后，恶意破坏或更改网页内容，使网站无法正常工作或出现黑客插入的非正常网页内容，造成不必要的经济和形象损失。2012年1月至11月，CNCERT监测的遭受网页篡改的网站数量如下图所示。



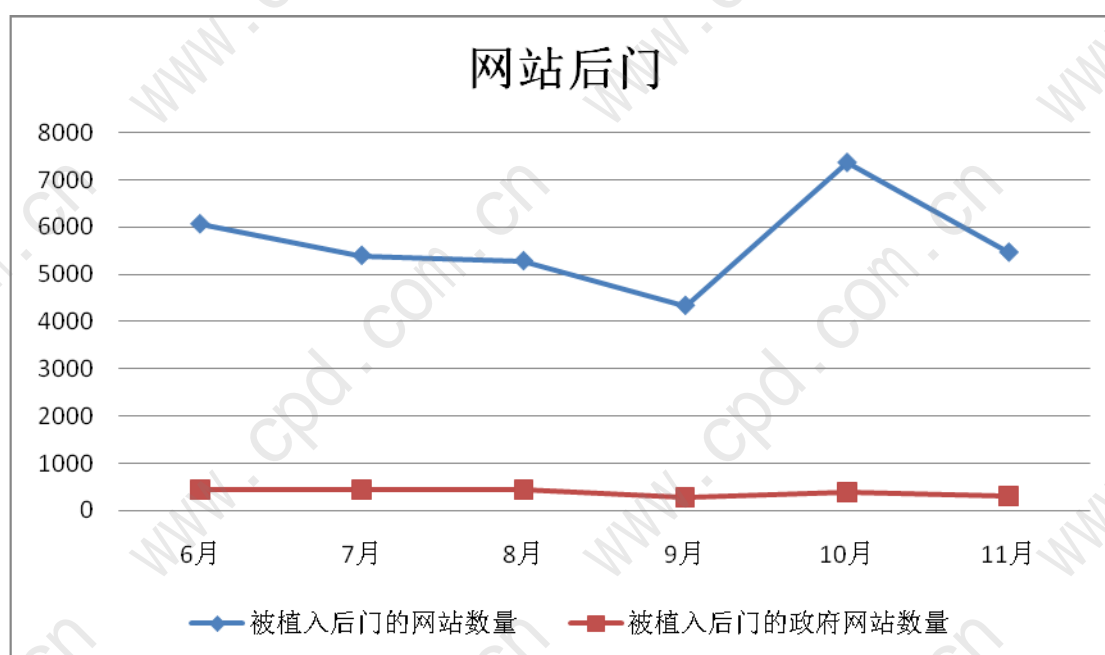
## ②网页仿冒

网页仿冒是通过构造与某一目标网站高度相似的页面（俗称钓鱼网站），并通常以垃圾邮件、即时聊天、手机短信或网页虚假广告等方式发送声称来自于被仿冒机构的欺骗性消息，诱骗用户访问钓鱼网站，以获取用户个人秘密信息（如银行帐号和密码）。2012年1月至11月，CNCERT监测的网页仿冒数量如下图所示。



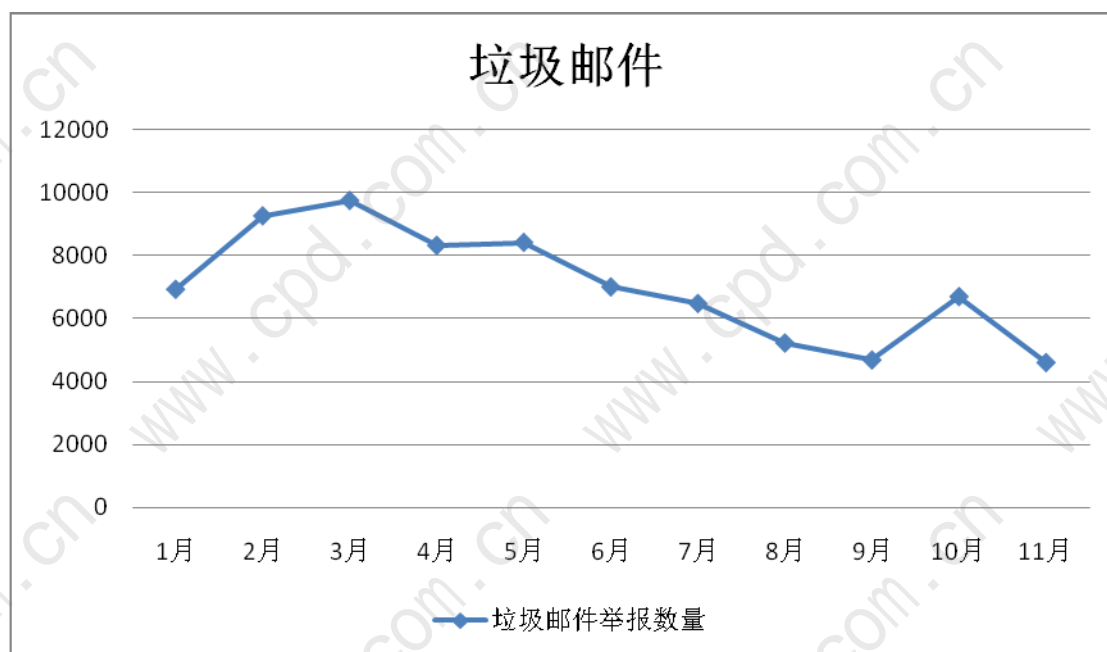
### ③网站后门

网站后门是指黑客在网站的特定目录中上传远程控制页面从而能够通过该页面秘密远程控制网站服务器。2012 年 1 月至 11 月，CNCERT 监测的网站后门数量如下图所示。



#### (4) 垃圾邮件

凡是未经用户许可就强行发送到用户的邮箱中的任何电子邮件。包括：(1) 收件人事先没有提出要求或者同意接收的广告、电子刊物、各种形式的宣传品等宣传性的电子邮件；(2) 收件人无法拒收的电子邮件；(3) 隐藏发件人身份、地址、标题等信息的电子邮件；(4) 含有虚假的信息源、发件人、路由等信息的电子邮件。2012 年 1 月至 11 月，中国互联网协会反垃圾邮件中心报送数据情况如下图所示。



#### 网络安全热点案例

##### (一) “火焰 (Flame)” 病毒

2012 年 5 月，卡巴斯基实验室发现一种破坏力巨大的全

新电脑蠕虫病毒“火焰 (Flame)”在中东地区传播，其中伊朗受病毒影响最严重。“火焰”病毒构造十分复杂，是一种全新的网络间谍装备。该病毒可以通过 USB 存储器以及网络复制和传播，并能接受来自世界各地多个服务器的指令。感染“火焰”病毒的电脑将自动分析自己的网络流量规律，自动录音，记录用户密码和键盘敲击规律，并将结果和其他重要文件发送给远程操控病毒的服务器。一旦完成数据搜集任务，这些病毒还可自行毁灭，不留踪迹。

## (二) Gauss 病毒

2012 年 8 月，卡巴斯基实验室又发现了类似“火焰”病毒的 Gauss 病毒，一个从事收集财务信息的间谍软件。它是出现在中东地区的一个新的网络间谍软件，可以窃取浏览器保存的密码、网银账户、Cookies 和系统配置信息等敏感数据。

## (三) “迷你火焰 (miniFlame)”病毒

2012 年 9 月，卡巴斯基实验室的研究人员发现了专门用于攻击大型公司的“迷你火焰 (miniFlame)”病毒。据悉，该种病毒的运作情况跟此前的 Flame 和 Gauss 非常相似。而 miniFlame 的出现似乎将这以上两种病毒联系在一起，甚至可以推测这两种病毒来自同样的开发者。病毒幕后团伙首先通过 Flame 窃取数据，然后再从中筛选大型公司，然后植入 miniFlame 这一病毒，从而获得更加详尽的数据信息。一旦



系统先后感染了 Flame 和 miniFlame 这两种病毒，攻击者就可以往相应的 PC 上发送被称为 browse32 的模块，然后从 PC 上删除掉 Flame 病毒，转而植入 miniFlame 病毒。比较有意思的是，miniFlame 具备拦截 Flame 再次被安装的功能。

#### （四）网络战攻击群

一些网络分析专家认为，有足够的证据表明，miniFlame、Gauss、Flame、“震网（Stuxnet）”等病毒有着密切的关系，因为 Gauss 似乎和 Stuxnet 病毒来自同一个国家，而 Stuxnet 病毒和最复杂病毒 Flame 关联紧密，miniFlame 模块其实是一个协作工具，可以作为一个独立的恶意程序使用，或者同时能够充当 Flame 和 Gauss 恶意软件的插件。这似乎已形成了“网络战”攻击群，Stuxnet 病毒攻击的是伊朗核设施，而“火焰”病毒攻击的则是中东石油部门的商业情报，Gauss 病毒攻击的是中东地区的金融机构和在线支付系统。Flame 和 Gauss 主要是窃取数据和信息，miniFlame 则是一个后门，它为操作者直接提供通向受感染机器的入口。

### 总结

伴随着云计算、物联网和移动互联网的迅速普及，2012 年网络信息安全事件此起彼伏，从安全漏洞到黑客攻击，从信息泄露到蠕虫施虐，网络威胁无处不在。展望 2013 年，可能会出现越来越多的针对消费者、企业和政府的针对性攻



击，并且可能会出现针对关键基础设施的网络战行为，也会出现新兴和复杂的移动威胁。

## （六）网络贩毒

早在 2001 年，联合国国际麻醉品管理局公布的年度报告就指出，利用因特网聊天室或者名义上只能出售处方药的网上药店进行的毒品交易正日益泛滥。近年来，随着网络、电子商务和物流的不断发展，通过网络联系买家贩卖毒品，并通过物流渠道进行贩运的案件越来越多。所谓的网络贩毒，实际上就是利用网络进行贩卖毒品的行为。

### 1. 我国网络贩毒概况

《第 30 次中国互联网络发展状况统计报告》显示，截至 2012 年 6 月底，中国网民数量达到 5.38 亿，增长速度更加趋于平稳；其中最引人注目的是，手机网民规模达到 3.88 亿，手机首次超越台式电脑成为第一大上网终端。<sup>①</sup>通过计算机网络、手机网络进行毒品贩卖的情况屡见不鲜，网络贩毒逐渐成为我国禁毒部门打击的重点。2012 年 2 月，济南警方破获了通过互联网络贩卖“冰毒”的案件；<sup>②</sup>2012 年 3 月，吉林警方查获一起横跨全国 18 个省市、涉案人员达 400 多人的特大网络贩卖毒品案，在这起案件中，QQ 等网络聊天工具、淘宝等网络交易平台成了贩毒、吸毒的“秘密通道”；

<sup>①</sup> 参见《第 30 次中国互联网络发展状况统计报告》。

<sup>②</sup> 济南警方侦破一起网络贩毒涉枪案：<http://news.qq.com/a/20121012/001634.htm>

<sup>①</sup>2012 年 4 月，贵州警方破获了被列为公安部目标案件的网络运输贩卖毒品案，抓获以胡某为首的嫌疑人 13 人，缴获冰毒 443 克、K 粉 175 克、麻古 10 克；<sup>②</sup>2012 年 7 月，重庆与山东警方联手摧毁一个利用互联网传授制毒技术并从事制毒犯罪团伙<sup>③</sup>。

上述对外公布的案件仅是冰山一角，鉴于我国网络监管体制混乱、网络贩毒情报工作基础薄弱的现实状况，大量隐性存在的网络贩毒案件尚未被公安禁毒部门掌握，日益严峻的网络贩毒问题已严重影响我国“陆海空邮”禁毒防控体系的运行效果。

## 2. 网络贩毒的特点

### (1) 隐蔽性强，不易被发现

网络空间的虚拟性决定了网络违法犯罪行为的隐蔽性。这一点在网络贩毒中体现的尤为明显，主要体现在以下三个方面：

第一，手法的隐蔽性。网络空间具有无形性，而网络贩毒一般是通过专业的软件运用相关的程序在这种无形的空间内完成的，这就决定了网络贩毒很难被外人发现。如行为人一般是通过专业的购物网站对伪装过的毒品进行交易，整个交易过程只需几个简单的操作就能完成。再者，行为人在

<sup>①</sup> 县级市竟有 30 多名青年吸毒 警方挖出跨 18 省网络贩毒案：

[http://www.legaldaily.com.cn/Political\\_work/content/2012-03/27/content\\_3462264.htm?node=35417](http://www.legaldaily.com.cn/Political_work/content/2012-03/27/content_3462264.htm?node=35417)

<sup>②</sup> 贵州黔南警方破获部督网络贩毒团伙案纪实：

[http://www.legaldaily.com.cn/Political\\_work/content/2012-07/09/content\\_3694249.htm?node=35417](http://www.legaldaily.com.cn/Political_work/content/2012-07/09/content_3694249.htm?node=35417)

<sup>③</sup> 渝鲁警方联手摧毁一利用互联网传授制毒技术并从事制毒犯罪团伙：

<http://legal.people.com.cn/n/2012/0703/c188502-18435668.html>

进行网络贩毒时所用到的数据或指令都是无形，而且能够证明行为过程的证据通常存储在有关的硬件或软件设备上，只要一个简单的操作就能完全销毁，使得行为人很容易转移或销毁证据。

第二，贩毒活动的隐蔽性。从时间来看，行为人在一天24小时的任何时间内都可以进行贩毒行为，不受时间长短、多少的限制。从空间来看，只要是在有电脑和网络的地点，无论是公共场所还是私人场所，行为人都可以进行贩毒行为，而且可以从头至尾都不接触被害人。

第三，贩毒过程的匿名性。网络空间是一个虚拟的空间，行为人在此空间内接受文字或图像信息的过程不需要任何登记，完全匿名。行为人在网络上进行贩毒行为不可能用真实姓名，而是用所谓的“网名”，而且一个行为人可能有两个甚至更多的“网名”，并且频繁更换进行贩毒行为，这就进一步加了查控的难度。

## （2）跨越区域空间大

据有关统计数据显示，全球互联网已经覆盖200多个国家和地区的6亿多人口，这使得世界变得越来越小。在网络虚拟空间中，没有现实世界的地域界线，因而行为人不仅可以在国内不同区域间进行交流，而且可以跨越国界进行国际间的往来。在网络贩毒中，无论买方是在本地还是异地，国内还是国外，贩毒者都可以通过网络与其交流，并在网上支

付货款。交易过程完全是通过网络进行，买方与卖方并没有现实的接触，看似复杂的过程通过简单的几个程序操作就完成了。

### （3）贩卖的毒品以合成毒品为主

利用网络进行贩卖的毒品通常是 K 粉、摇头丸等合成毒品。所谓的合成毒品是相对鸦片、海洛因等传统毒品而言，由人工化学合成的致幻剂、兴奋剂类毒品，是由国际禁毒公约和我国法律法规所规定管制的、直接作用于人的中枢神经系统，使人兴奋或抑制，连续使用能使人产生依赖性的精神药品（毒品）。合成毒品大多为片剂或粉末，便于携带和贩运；吸食者多采用口服或鼻吸式进行吸食，不易被察觉，而且制售渠道繁杂，管理难度较大，这使得网络很自然的成为合成毒品蔓延的媒介。

### （4）涉案主体多为青少年

从公安机关抓获的犯罪嫌疑人来看，35 岁以下的青年占 66.2%，18 岁以下的青少年占 2.6%。这一方面由于青少年自身的心智尚不成熟，出于好奇、追求刺激等原因而误入歧途；另一方面，由于网络在青少年群体的普及，大多青少年将自己置身网络虚拟空间，做自己喜欢做的事情，以逃避各种现实的不快。

## 3. 典型案例

### 济南 2·15 贩毒案

2012 年春节前夕，济南市公安局禁毒支队侦查员获得线索，一个网名为“冰刀”的人，意图通过互联网络联系下家到济南贩卖“冰毒”。缉毒警察认真地对“冰刀”贩卖毒品的线索进行了长达一个多月的侦查监控工作。

2 月 13 日，侦查员得到确切情报，“冰刀”将于 2 月 14 日左右携带毒品到济南与下家进行交易。禁毒支队的侦查员在随后的两天里进入了临战状态，为抓捕工作做好了准备。但是“冰刀”却似乎钻入了地下，连续两天没有动静。2 月 15 日中午，“小雨”和方某携带毒品从淄博驾车到达济南。按照抓捕预案，侦查员们在毒贩入住的旅馆房间内进行抓捕，一举抓获毒贩，缴获毒品。

经过侦查，警方发现“冰刀”实际另有其人，就是藏身淄博的曹某。济南缉毒警察随即赶赴淄博，将毒贩曹某抓捕归案，同时落网的还有一名叫刘某的人。经查实，曹某和刘某都是刚毕业的大学生，没能抵制住诱惑，寻求刺激而吸毒，后来参与贩毒，经常在网上联络贩毒。这次，曹某让“小雨”和方某到济南贩卖毒品。

## （七）网络制假售假

### 1. 网络制假售假泛滥的成因与特点

#### （1）背景

①艾瑞咨询数据显示，2012 年前三季度中国网络购物市场交易规模为 7807.7 亿元，超过 2011 年 7665.8 亿元的全

年交易额，占中国前三季度社会消费品零售总额的 5.2%。

②2012 年 12 月 3 日，阿里巴巴集团宣布，截至 2012 年 11 月 30 日，本年度集团旗下淘宝和天猫交易额突破 10000 亿元。

③2012 年 11 月 11 日，天猫与淘宝大促，日交易额达到 191 亿元，远超此前预期的 100 亿元目标，且超过 2012 年美国“网购星期一”（Cyber Monday）的 15 亿美元水平。

④根据深圳《晶报》调查，目前淘宝网网上的假货比例超过三分之一，品种几乎涵盖了淘宝所有线上在售的商品，其中尤以化妆品、手机、服装、鞋子和珠宝首饰类为多。从中可以看出网络售假呈现品种多、数量大，且均依托网店进行公开的售假行为，销售范围广。

## （2）网络假货范围

按照产品是否侵犯其他正牌商品的知识产权，可以将网络假货划分为三个层次：①侵犯知识产权的假冒伪劣商品，如山寨货；②非正品：如仿货、水货；③与事实描述不符的商品，如被虚假宣传所美化的产品。

## （3）特点

①交易平台多样化。在一系列严惩侵犯知识产权和制售假冒伪劣商品犯罪专项整治活动后，不法分子转而选择一些外贸交易平台或自建网络平台实施侵犯商标类犯罪，仿冒国内外知名品牌逐渐成为主要犯罪类型。

②犯罪主体复杂化。侵犯知识产权和制售伪劣商品犯罪趋向专业化、产业化、链条化，犯罪主体从以往自然人为主，逐步向公司法人组织转变，且犯罪数额大、涉案人数多，有专人从事进货、发贴、网聊、送货等违法活动。

③被告人技能专业化。网络销假被告人文化程度相对较高，由对法律无知向漠视法律或侥幸心理转变。

④销假查证困难化。被告人往往采取付费聘人点击增加信誉度，虚拟交易缺乏明确指向性。即便查获其网上销售的假冒商品，网页商标截图与真品商标的比对也存在困难。

## 2. 网络制假售假的主要门类

### (1) 假证、假印章

公安部集中全国各地警方力量，截至 2012 年 7 月，先后捣毁了 118 个涉案从事制贩假证、黑客入侵窝点，165 名犯罪嫌疑人落网，收缴虚假证书超过 12 万本，虚假印章超过 1 万枚。据不完全统计，共有 180 多个政府人事网站被黑客入侵，300 多万条涉及个人隐私的资料被盗卖，3 万多人办理各类假证的数据，涉案金额 3 亿多元。

### (2) 假烟假酒

江西省鹰潭市公安局月湖区分局从一家名为“多克龙”的网店入手，历时近 2 个月，侦破一起案值金额高达 4000 余万，涉及 25 省的特大网络销售假酒案。

湖北省十堰市公安局破获了一起被公安部、国家烟草专

卖局列为督办案件的制售假烟案，捣毁了共计 7 个制假窝点，抓获犯罪嫌疑人 28 人，查获涉案违法人员共计 68 人。涉案金额达 1.44 亿元，销售网络遍布河南、云南、黑龙江等 16 个省市区。

### (3) 假药

浙江省台州市玉环县警方成功破获一起利用淘宝网店铺平台制售假药大案，现场查获假冒减肥产品 5 万余盒，涉案金额高达数千万元，并相继联合苏、粤、豫、冀等多地警方共同开展跨省集群战役，将此售假网络一举摧毁。而就是这家大规模出售假药的店铺，居然还是淘宝网的“三皇冠”。

甘肃白银和广东广州两地警方成功破获了一起由公安部督办的罗某涉嫌利用互联网销售假药一案，抓获犯罪嫌疑人 2 人，查获坐骨神经痛丸等假药 40 余个品种、180 余件，经初步调查可确定的销售额达 1000 余万元，并关闭非法销售和宣传药品信息的网站 6 个，摧毁了销售假药的窝点和网站。

### (4) 假生活用品

南宁市公安局青秀分局经侦大队与工商联手端掉一个化妆品制假售假窝点，查获涉假化妆品 6 货车，涉及 190 个品牌的 515 个品种，涉案金额 300 万元。

10 月底，福建马尾警方展开统一收网行动，出动近百名警力，抓获犯罪嫌疑人 14 名，查获大量假冒耐克、阿迪达斯、李宁、彪马、匡威等品牌各类运动鞋、运动服近万双



(件)，涉案金额达 2000 多万元。

从政府市场监管职能看，网络商品交易及有关服务行为监管涉及公安、工商、质监等多个职能管理部门。在互联网犯罪方面，只有符合构成刑事犯罪且涉案金额较大的案件，公安机关才受理，其余仍主要由工商、质监等行政主管部门负责受理。然而这些部门在网络打假方面仍是“各自为战”。要有效打击网络售假，就必须建立上下畅通、内外互动的常态化工作协调机制；加强对单个网民投诉的受理力度。单个网民的投诉涉及金额较小，但积累起来影响面较广。

## **(八) 网络贩枪**

### **1、网络贩枪的成因**

#### **(1) 需求增大**

中国拥有大量的枪械爱好者，尤其是近年来随着 CS（反恐精英）类游戏的盛行，更是培养出了一批军事发烧友和枪迷，这些枪支爱好者有一些共同的特点，文化层次比较高，有相对稳定的工作，收入不错，有些甚至对枪械到了几乎痴迷的程度。因此对于他们来说，从一些期刊杂志或军事网站上通过图片的方式获得对枪支的一些视觉体验已不能满足他们对枪支的爱好，他们更希望拥有一把实物枪支甚至于通过枪支射击获得快感，这些枪迷们便成为了当前持有仿真枪的潜在人群，而且随着人们收入水平的提高，这个群体在不断增大。但是在中国全面禁枪政策下由于无法购买真枪，于

是大批枪迷转而通过各种途径购买仿真枪来满足自己的兴趣爱好，对仿真枪的需求形成了一个巨大的买方市场，由此涌现出了一批暗藏在地下的黑色产业链，网络贩枪问题随之产生。

## （2）规避管制

《枪支管理法》明确规定禁止制造、销售仿真枪，于是大量不法商贩为了规避管制通过各种隐蔽手段贩售仿真枪，尤其是近几年随着网络购物的快速发展，网络贩枪成为了贩枪者最主要的贩枪途径。在网上贩枪者多使用网络贩枪暗语，如“出售单发手狗，左轮双动式，气体直接压入弹壳发射，跟真狗弹一样……”等等广告语，仿真枪在销售时被冠以多种代号，例如“狗”、“鸡”等，或者将型号、类型加到名称中，如“德国 586 左轮气手狗”等等。同时为了避免身份暴露，贩枪者将交易地区和联系方式均采用了复杂难懂的代号。而仿真枪的买方通常在网络上留下自己的手机号、QQ 号或 MSN 号，公布自己需要的枪支型号，对对方的真实身份一般不做核实。只要交易谈妥，卖方通过物流发货，买方通过网上银行付款。这种网络交流、交易的非接触式犯罪，正使其成枪支买卖的“温床”。

## （3）暴利驱使

由于枪支贩卖的暴利超贩毒，使犯罪分子铤而走险，并吸引了网上从事此类交易的买家也纷纷涌入这个领域。比如

2012 年 5 月份深圳警方破获的“特战营”一案中，原价 1000 元左右的高仿真枪，嫌疑人何某叫卖的价格一般为 2000 多元。也就是说，做成一宗买卖能赚一倍差价<sup>[1]</sup>。2012 年 4 月，青岛市公安局刑警支队会同城阳分局抓获的一特大网络贩枪团伙中，据嫌疑人王某交代，购进一支气手枪的价格在 3500 元到 5000 元之间，经过改装，每支加价 5000 元到 8000 元不等，改装后的仿真六四手枪每支能卖到 15000 元到 20000 元。经他转手后，每支枪可以获利六七千元。所以，后来他干脆辞掉了会籍顾问的工作，专门从事网上贩卖枪支<sup>[2]</sup>。在这些贩卖枪支的嫌疑人当中，还有一部分人原先是 CS 真人对抗游戏的爱好者，在接触枪支过程中，发现贩卖枪支的利润可观，渐渐走上了犯罪道路。

## 2、2012 年网络贩枪的特点分析

### (1) 交易方式隐蔽

犯罪分子为了逃避公安机关的查处，在网上销售仿真枪时设计了“暗语”。他们网上联系时常以“狗”代称枪支，长枪叫“长狗”，手枪叫“短狗”，气枪称为“气狗”，枪管称为“毛瓦”，“米”或“粮”则特指子弹，“秃鹰”气枪称为“秃子”等等。而具体指某一款型号的仿真枪时，则会通过业内的术语来传达信息。比如，在网上发布“654K”，买家一看就会知道这是一款仿真枪型号。同时他们一般都会在一些军事网站、狩猎论坛上寻找买家，并通过淘宝、拍拍等

平台交易，或者对有意购买者转到 QQ 私聊，之后买家把货款通过银行转账等方式打到指定的账号，卖家见钱发货。为了避免身份暴露，有些犯罪分子在网上还购买别人的银行卡用来收钱。

与此同时，犯罪分子还通过快递包裹的形式接货和送货。在货单上常用手机、PSP 游戏机、机械零件等其他物品名称代替。有的犯罪分子为了掩人耳目，选择将枪支的零部件分开送货，即使送货过程中被发现，只看一样零部件，根本不会发现什么，只有把所有零部件组装起来，才是一支完整的枪支。这些都增加了警方侦查的难度。

## （2）涉案人员多、地域跨度大

贩枪团伙为了扩张生意会不断发展下线，而且由于网络贩枪确实暴利可图，导致很多人都纷纷涉足到该领域中，同时也由于电子商务的发展和快递业的繁荣，贩枪团伙可以把他们的枪支销往全国各地。2012 年破获的几起重大的网络贩枪案都体现了这个特点。如 2012 年 6 月 12 日，浙江台州警方成功侦破的一起公安部督办的网络贩卖枪支案件中，抓获涉案嫌疑人 248 名，此案涉及的人员多，层级也多，总共有六七个层级，并且地域跨度非常大，办案民警花了 2 个多月的时间，从全国各地提取到涉案的数十万条网络交易数据。同时，民警花了大量的精力去伪存真，才把网上贩枪交易过程梳理清楚，共梳理出 1000 多名涉案人员的信息情况并展

开调查，可以说是网撒全国来抓捕犯罪嫌疑人<sup>[3]</sup>。而在江西省萍乡市公安局主办的“9·27”特大网络贩枪案中，贩枪团伙的买家遍布全国除西藏和港澳台地区以外的30个省市自治区，涉及212个地市州，400余人<sup>[4]</sup>。2012年9月，公安部直接指挥破获的“7·19”特大网络贩卖枪支弹药案，则抓获了犯罪嫌疑人530余名<sup>[5]</sup>。这是公安部组织开展缉枪治爆专项行动以来破获的又一起网络贩枪大案。

### （3）买主多为中高收入人群

由于中国境内的仿真枪除了少部分低档仿真枪由国内一些玩具厂商制造外，大部分仿真枪支的生产地均在境外的台湾、香港、日本等地，通过走私方式进入大陆地区。同时由于国内无国家认可的正规市场存在，走私到中国境内的仿真枪在价格上会比境外贵好几倍，比如一支“秃鹰”气枪标准配件，网络售价近万元，这决定了买仿真枪的人员绝大多数具有不错的经济收入，他们有些是狩猎爱好者，比如一些私营企业主，有钱又有闲。如在江西省萍乡市公安局主办的“9·27”特大网络贩枪案中，上海购枪者龚勇军曾开过煤矿，资产据称上千万，龚被捕时正身着迷彩服，扛着枪准备外出打猎<sup>[4]</sup>。有些则是有正当职业和固定收入的城市白领，这些枪械“发烧友”往往不满足拥有一支气枪，有的甚至会采购两支甚至更多，一些枪迷还会补充采购激光测距仪、瞄准器、消声器等配件，以满足个性化需要。他们都知晓持有

和买卖如此具有杀伤力的仿真枪属于违法行为，但自称无法抵御枪支带来的新奇诱惑。近年来已发生很多起因购买仿真枪而被判刑的案例。

## （九）网络恐怖活动

信息技术的发展引领了大数据时代的潮流，人们对于网络的依赖性逐步增强。据中国互联网络信息中心发布的《第30次中国互联网络发展情况调查统计报告》，截至2012年6月底，中国网民数量已达到5.38亿，互联网普及率已达39.9%。<sup>①</sup>强大的使用基数及宽松的网络环境为恐怖主义活动提供了温床，滋生出了一种新型的危害国家安全和影响社会政治稳定的恐怖活动——网络恐怖活动。笔者在对相关资料进行了系统的梳理与分析的基础上，对2012年网络恐怖活动的概况做出了总结，以期为公安工作乃至相关工作的开展提供一定的参考和借鉴。

### 1. 2012年网络恐怖活动案例

网络恐怖活动是指个人或组织在网络空间内进行的，并希望通过破坏性效应制造恐怖气氛来达到某种明确的政治、宗教或意识形态的目的。<sup>②</sup>笔者运用百度、Google、360、必应等搜索引擎对2012发生的网络恐怖活动进行了搜集与梳理：

（1）末日说。自2012年年初以来，网络上关于2012年12

<sup>①</sup>中国互联网络信息中心. 第30次中国互联网络发展情况调查统计报告[J].

<sup>②</sup>王高阳. 国际关系理论视域下的网络恐怖主义分析[J]. 重庆: 重庆交通大学学报, 2012(10).

月 21 日为世界末日的谣言一直未曾停止过。在这些舆论的渲染下，许多民众信以为真，采取了抢购蜡烛、抢购食物、变卖家产等行为，末日网络营销也“应运而生”。

(2) 太阳风暴袭击地球事件。网络传言，2012 年 9 月 22 日美国纽约曼哈顿出现极光现象，接下来的一年内地球会面临灾难，引起许多民众的惶恐。

(3) 新疆恐怖分子利用网络进行恐怖犯罪活动。2012 年 8 月初，新疆维吾尔自治区法院依法对 5 起利用互联网、移动存储介质，进行组织、领导、参加恐怖组织和煽动分裂国家的犯罪案件进行了审理。

(4) 十八大会前的“封网”事件。网络传言，十八大期间要封网限制舆论，引起网民对政府的不满。

(5) 网络中出现恐怖网站。恐怖网站散布恐怖图片、恐怖故事和恐怖视频，充斥着暴力、死亡等元素。

(6) 中国篮协网站被日本黑客袭击，发布“钓鱼岛属于日本”的言论。

(7) 雅虎服务器被黑，45.3 万份用户信息遭泄露。

## 2. 网络恐怖活动的分类

从国内已有的网络恐怖案例来看，网络恐怖活动大致可以分成以下几种<sup>①</sup>：

---

<sup>①</sup>樊彦芳. 利用型网络恐怖犯罪是当前网络反恐重点[J]. 北京: 中国社会科学报, 2012(9).

(1) 攻击计算机和网络系统。随着信息化时代的到来，人们在生产、生活、工作方面越来越多的依赖网络，但是这方面的网络防护能力却相对薄弱，易成为恐怖分子的袭击目标。如中国篮协网站被黑事件。

(2) 攻击数据信息。随着大数据时代的到来，数据信息的作用越来越大。而利用网络窃取信息，已经成为恐怖分子的手段之一。只要有网络，那么数据攻击事件就每天都在发生着。如雅虎服务器被黑事件中，45.3万份用户信息遭泄露。

(3) 利用计算机网络实施恐怖活动。

①网络恐怖思想宣传。利用网络达成对人们心理空间的威慑和打击。如末日说，导致民众产生恐怖情绪，如抢购蜡烛、卖房借钱捐款、小女孩不肯上学等。

②传授犯罪方法。如经公安部认定公布的第二批、第三批恐怖人员名单中，就有不少“东伊运”恐怖分子将制作爆炸物的技术和方法上传互联网，教唆组织成员下载学习的犯罪事例。

③组织恐怖活动。如新疆今年发生的5起利用互联网、移动存储介质，进行组织、领导、参加恐怖组织和煽动分裂国家的犯罪案件。

④散布虚假恐怖信息。网络可以轻易的传播谣言和虚假信息，在事情未得到证实之前，恐怖分子可以先散布有利于



己的信息，抢占舆论先机，还可以利用图片、视频等肆意歪曲事实。如末日说的传播与渲染。

### 3. 网络恐怖活动的特点

网络恐怖活动与传统的恐怖活动相比，具有以下几点特点：

(1) 与传统的恐怖活动相比，网络信息传播更便捷迅速。网络具有极强的时效性，打破了时空对恐怖活动的限制，恐怖分子可以在第一时间内组织、策划、控制恐怖活动。

(2) 涉及面更广。据中国互联网络信息中心发布的《第30次中国互联网络发展状况统计报告》，中国网民规模不断扩大，手机成为网民的第一大上网终端<sup>①</sup>，即使是在经济欠发达的偏远地区，手机上网也已成为可能。因此，网络恐怖活动的范围十分广泛，从国外到国内，从发达城市到欠发达山村都可涵盖。

(3) 资金消耗低。目前，我国上网费用并不高，而且手机上网也十分方便，恐怖分子组织活动可直接通过网络进行联系与沟通。相比以前，资金消耗十分低廉。

(4) 操作难度小。网络的产生和技术的发展，使得恐怖分子只需在世界的一角，轻轻按下键盘就可发动一起恐怖活动。

---

<sup>①</sup>李本先 李孟军 孙多勇 迟妍 范林军. 社会网络分析在反恐中的应用[J]. 复杂系统与复杂性科学, 2012(6).

#### 4. 网络恐怖主义的发展趋势

近些年来，网络恐怖活动无论从数量规模还是到危害程度都不断升级，已对国家安全构成严重危害。笔者认为，要想更好的维护网络安全，就需要了解网络恐怖主义的发展趋势：

(1) 行动更隐蔽。由于网络技术监控和网络舆论导向的难度较大，因此网络恐怖活动更具隐蔽性。

(2) 防范更困难。网络技术的发展以及网络活动的隐蔽性加大了网络恐怖活动的防范难度。黑客可能成为实施网络恐怖主义的工具，据统计，当今世界上平均每20秒就有一起“黑客”事件发生。美国每年由此造成的经济损失超过100亿美元。<sup>①</sup>

(3) 攻击更有效。当一个恐怖组织网络被攻击后，组织网络中的人员被打散，但网络中的某一个群体，如果有足够的资源去发动恐怖袭击，那么即使是网络中的核心人物被捕，其他成员一样可以按照计划进行作战。即使是单个的恐怖分子，如果他手中掌握了足够的信息、物质资源、任务计划，那么单个人同样可以发动一定规模的恐怖袭击。<sup>②</sup>

(4) 后果更可怕。自2012年起，恐怖活动可能会主要锁定那些对一个国家国民经济或人民生活有着巨大影响的大

---

<sup>①</sup>奇云.网络恐怖主义——没有硝烟的战争[J].观察与思考,2012(3).

<sup>②</sup> tangxs.网络恐怖主义成为黑客的第四支力量[J].网络与信息,2012(4).

型基础性设施，如通信系统、金融行业、电力设施、供水系统、油气能源、机场指挥中心、铁路调度、军事装备等。一旦此类恐怖活动成功，其对国家造成的危害将是巨大的。

(5) 网络恐怖分子可能成为继经济驱动、黑客主义和国家间谍行为之后的第四种互联网攻击者。“互联网可以充当恐怖分子的电视、广播电台，或者国际报纸和期刊。网络允许对事件未经审查和过滤的描述在全球传播。聊天室、网站和电子公告在很大程度上不受控制。这种环境对于资金缺乏的组织解释其行为或者抵消其国内外的谴责非常理想。”<sup>①</sup>

总而言之，网络已经成为恐怖主义进行恐怖活动的新型媒介，如何在未来做好网络安全的防范与保护是摆在我们面前的一个十分现实而又十分艰难的课题。

### 三、中国互联网违法犯罪预防对策

#### (一) 网络违法犯罪防治的难点

##### 1、打击防范存在“时滞”

互联网络的技术和应用服务创新周期短，传播扩散速度快。当多数人还在尝试接触和使用新网络应用时，具有违法犯罪动机的人就已经开始使用闻所未闻的新形式或手段实施违法犯罪行为。不管是公众的防范意识，还是社会控制机构的重视程度、技术应对和打击措施都存在明显的“滞后

---

<sup>①</sup> Thmothy L. Thomas, Al Qaeda and the Internet: The Danger of “Cyberplanning”, p. 114, <http://www.carlisle.army.mil/... /thomas.pdf>

性”。网络违法犯罪常常呈现“先爆发，后治理”的局面，预先防范的难度极大。

## 2、犯罪证据提取困难，证据效力容易出现争议

由于网络违法犯罪发生在以网络硬件和软件为物理和技术基础的虚拟空间，难以追查行为人的真实身份和实际处所。相关违法犯罪行为的痕迹或多或少表现为电子信息的形式，违法犯罪证据容易销毁，证据的提取要求有较高的信息和网络技术支持，电子数据证据的真实性和关联性在实践中很容易引发争议。这些都为依法打击网络违法犯罪增加了难度。

## 3、犯罪管辖权确定与侦查区域合作操作困难

由于互联网络具有超时空的特性，网络违法犯罪行为主体、行为发生地与现实社会的物理空间之间的关系具有多重性，其管辖权的认定上存在难度。在当前我国犯罪侦查工作“条块分割”的体制下，关于在何地立案的问题常常找不到具体明确的依据。即使顺利立案，原有的各部门的配合和协作机制也常常无法满足网络犯罪案件具体侦查工作的需求。

## 4、相关法律不完备

原有的法律法规大多是针对现实社会中的违法犯罪行为制定的，即使近年来我国出台了一系列与互联网络有关的专门法律法规和相关司法解释，仍远不能满足打击网络违法犯罪工作的具体要求。立法层次低，多头立法，多头管理，

协调性较差、具体操作性不强，法律效率较弱，立法及调整速度远远落后于新的网络技术和应用性网络服务所引发的违法犯罪事实。

## 5、跨国网络犯罪打击查处难度大

网络违法犯罪行为充分利用了互联网络“无国界”这一特点，大量采用跨国犯罪的形式来实施犯罪行为。由于很多情况下不同国家对于犯罪的法律定义不同，打击网络跨国犯罪时只有相关行为同时触犯两国法律，才有合作的基础。同时，在打击成本和协调机制上都存在不小的难度。

## （二）网络违法犯罪防治机制建设

网络是一个与现实社会有着复杂关系，同时又具有超时空性、虚拟性、匿名性、反控制等独特性的综合系统。网络违法犯罪防治体系的构成要素主要可以分为：针对互联网络的法律法规、网络司法执法主体、网络越轨主体、网络硬件（软件）服务提供商、网络技术及应用、网民、网络文化和现实社会大环境等八个方面。

网络违法犯罪的防治机制建设就是正确处理好这八个要素之间的关系，使其各司其职，相互促进，协调运作。具体可以分为三个部分。一是“硬件”机制建设，强化网络执法主体力量，在人力、财力、技术、装备等方面加强打击力量；合理规范、引导网络服务提供商的权利、义务，击破非法利益链条；严打网络违法犯罪主体。二是“软件”机制建

设，建立健全网络法律法规，制定专门法；实行网络技术及应用创新报备制度和风险自查制度；大力开展积极向上的网络文化建设，树立正确健康的网络价值观念和道德伦理；提升网民的防范意识、法治意识，强化公众的“免疫力”。三是抓住网络违法犯罪的现实根源这个关键点，从现实社会问题治理入手消除种种不良现象和罪恶根源，从而净化网络空间。

### **（三）网络违法犯罪防治主要对策**

#### **1、“标”、“本”兼治，重在治“本”**

网络违法犯罪是现实社会犯罪因素在网络上的反映，其根本和源头在现实社会。要及时有效地解决好现实社会运行中的各种问题、紧紧抓住“网络违法犯罪行为人最终一定是现实社会人”这一关键、在可能的条件下适当实现部分网络越轨行为的“非罪化”。

#### **2、立法为先，集中打击**

加快网络领域的立法并予以完善，是防治网络犯罪的关键一步。要重视法律理念的虚拟空间转向、制定关于互联网的专门法、及时出台专项司法解释，只有这样才能使执法机关在预防打击网络犯罪行为时有法可依，严厉制裁，违法必究。由于网络犯罪被查处、有效打击的比例小，犯罪成本太低，客观上造成虚拟空间匿名状态下的越轨者的肆无忌惮。要形成打击网络违法犯罪的“兵力”优势、高压态势，

提高犯罪成本、警示公众。

### 3、多主体整合打击利益链条，形成防治合力

防治和打击网络违法犯罪不能仅仅依靠公安机关的力量，要切实联合网络硬件生产商、网络基础服务提供商、网络应用服务提供商、网民等众多互联网产业主体共同努力，积极配合，切断网络违法犯罪的黑色利益链条，形成防治合力。

### 4、“软”、“硬”兼施，抢占技术制高点

打击技术型网络犯罪，是与犯罪行为人在技术创新和时间上的一种赛跑。在硬件技术上应由社会控制部门前期介入；在软件上要加强侦查、监控工具的科研创新，通过完善防火墙技术、数据加密技术、网络扫描监控技术、网上监控、入侵检测、案件跟踪、灾难恢复等网络安全技术，强化“科技防治”的能力。

### 5、加强宣传，提升公众识别、防范能力

与传统犯罪相比，目前公众对网络犯罪(如网络诈骗)的防范意识严重不足。普及网络法律知识，加强预防网络犯罪的宣传教育，让广大网民在网络应用中时刻保持警惕，降低其成为犯罪受害人的可能性。

## 四、中国互联网违法犯罪治理的法治化

### (一) 当前我国在网络安全立法方面面临的问题

我国计算机安全法律体系主要由国务院及相关部门颁布的

法规和规章组成，法律层级较低，约束力较弱，执法范围较窄，缺乏系统性，存在法律空白和盲点，导致执法机关普遍处于管理难、举证难、执法难的境地。现行法律和规章滞后于互联网的发展，基本停留在“原则性”方面，实用性、操作性不强，与虚拟社会管理和网上打击违法犯罪实际需要有较大差距，达不到有效管理，威慑、打击犯罪的效果。从公安机关执法实践看，相关主体存在责权不统一的问题，网络案件管辖权限界定不清，网络虚拟财产认定缺乏法律依据，电子证据的勘验、鉴定缺乏有效法律支撑。

## （二）互联网违法犯罪防治的中国法律现状

针对互联网违法犯罪日益严重的现状，中国也在立法层面采取了不少应对措施：

### 1. 法律

目前中国遏制互联网违法犯罪的法律主要有：

（1）《刑法》及《刑法修正案（七）》。1997年刑法第285条第1款规定了非法侵入计算机信息系统罪，第286条规定了破坏计算机信息系统罪两个罪名，第287条规定：“利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的，依照本法有关规定定罪处罚。”2009年2月28日《刑法修正案（七）》第9条新增了非法获取计算机信息系统数据、非法控制计算机信息系统罪和提供侵入、非法控制计算机信息系统程序、工具罪两个罪名。



(2) 2000 年 12 月 28 日通过的《全国人民代表大会常务委员会关于维护互联网安全的决定》。该法律根据制裁后果的不同,将互联网不法行为区分为犯罪行为 and 一般违法行为;根据行为类型的不同,将互联网不法行为区分为妨害互联网运行安全的行为、妨害国家和社会稳定的行为、妨害社会主义市场经济秩序和社会管理秩序的行为、侵犯个人、法人和其他组织的人身、财产等合法权利的行为以及其他不法行为五类。

(3) 2005 年 8 月 28 日通过的《治安管理处罚法》。该法第 29 条规定,可以对五种妨害计算机信息系统安全的行为予以 5 日以下拘留或者 5 日以上 10 日以下拘留的行政处罚。

(4) 2012 年 12 月 28 日《全国人民代表大会常务委员会关于加强网络信息保护的决定》。明确了网络服务提供者的义务,加重了网络服务提供者的法律责任,从信息的搜集、整理以及信息的使用等各个方面,全方位地保护能够识别公民个人身份和涉及公民个人隐私的电子信息。第一,实行网络实名制。网络服务提供者为用户办理网站接入服务,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服务,应当在与用户签订协议或者确认提供服务时,要求用户提供真实身份信息。第二,规定网络服务提供者保护公民个人信息的义务,不得非法收集、出售、非法向他人提供、非

法使用。第三，将发送垃圾电子信息规定为非法行为。任何组织和个人未经电子信息接收者同意或者请求，或者电子信息接收者明确表示拒绝的，不得向其固定电话、移动电话或者个人电子邮箱发送商业性电子信息。第四，赋予网络服务提供商信息审查义务。要求网络服务提供者应当加强对其用户发布的信息的管理，发现法律、法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取删除等处置措施，保存有关记录，并向有关主管部门报告。第五，将“关闭网站、禁止有关责任人员从事网络服务业务”作为行政处罚的手段，并且将网络服务提供者违法行为“记入社会信用档案并予以公布”。

## 2. 行政法规

国务院颁布的有关行政法规有：1994年2月18日《计算机信息系统安全保护条例》、2000年9月25日《互联网信息服务管理办法》、2002年9月29日《互联网上网服务营业场所管理条例》等等。

## 3. 部门规章

主要有：1997年12月16日公安部颁布的《计算机信息网络国际联网安全保护管理办法》、2000年11月6日信息产业部颁布的《互联网电子公告服务管理规定》、2003年5月10日文化部颁布的《互联网文化管理暂行规定》、信息产业部2004年11月5日颁布的《中国互联网络域名管理办

法》、2005年12月13日公安部颁布的《互联网安全保护技术措施规定》、2006年6月20日信息产业部颁布的《互联网电子邮件服务管理办法》；等等。

#### 4. 法律解释

主要有：2004年9月3日《最高人民法院、最高人民检察院关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释》；2010年1月18日《最高人民法院、最高人民检察院关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释（二）》；2012年12月20日《最高人民法院关于适用〈中华人民共和国刑事诉讼法〉的解释》第2条第2款对网络犯罪的属地管辖作出了规定：“针对或者利用计算机网络实施的犯罪，犯罪地包括犯罪行为发生地的网站服务器所在地，网络接入地，网站建立者、管理者所在地，被侵害的计算机信息系统及其管理者所在地，被告人、被害人使用的计算机信息系统所在地，以及被害人财产遭受损失地。”

### （三）互联网违法犯罪防治的境外法治经验

#### 1. 国际公约

经过两周高密度磋商，国际电信世界大会于2012年12月14日在阿联酋迪拜闭幕，会议通过了修订后的《国际电

信规则》。在签字仪式上，有 89 个国际电信联盟成员在新《规则》上签字，55 个保留签字权。新《规则》将于 2015 年 1 月 1 日起实施。中国代表团认为，该规则符合目前国际电信现状并反映了发展中国家的诉求。但新《规则》条款内容仍遭到部分国家抵制。美国、英国、加拿大等国拒绝在新条约上签字，部分欧洲国家则持保留意见。主要分歧在于国际电信联盟是否支持政府对互联网企业的监管；条约是否应涉及网络安全和允许对垃圾邮件进行监控。

## 2. 外国立法

2012 年 7 月俄罗斯议会通过了《关于保护儿童免受损害健康和发展信息的联邦法律及其他法令》，于 2012 年 11 月 1 日起施行。法案规定传播对儿童有害内容的网站、网页的网址、域名将被列入黑名单。传播儿童色情、毒品、诱导儿童自残内容的网站将可能在法院裁定前即被列入黑名单并被关闭，而传播其他禁止发布的信息的网站将在法院裁决后决定是否被关闭。2012 年 10 月 15 日新加坡国会通过《个人资料保护法》，对违法发送垃圾信息等违法行为规定了罚款等处罚。2012 年 12 月 21 日，法国颁布《安全与恐怖主义法》，根据该法律，如果一名法国公民在国外接受极端主义思想灌输，即使他不是法国本土长大，在法国也没有违法行为，也能以恐怖主义罪名被判处可高达 10 年监禁和 22.5 万欧元

的罚金。该法案规定执法部门可以对可疑分子进行电话监听和分析其上网记录。

### 3. 我国台湾地区

我国台湾地区于 2010 年 05 月 26 日通过《个人资料保护法》（由原《电脑处理个人资料保护法》修改而来），但因为部分条款存在争议，直到 2012 年 10 月 1 日才得以在修正后施行，对侵犯个人资料的行为规定了包括刑罚在内的制裁措施。将基于公益需求的“人肉搜索”个人资料规定为合法，但是超出公共利益范围的则要承担法律责任。

### （四）互联网违法犯罪防治的法治完善建议

针对我国日益严重的互联网违法犯罪，应对尽快采取以下三个方面的法律应对措施：

#### 1. 制定互联网管理的综合性基本法律

目前我国互联网管理没有一部综合性的基本法律。《全国人民代表大会常务委员会关于维护互联网安全的决定》和《全国人民代表大会常务委员会关于加强网络信息保护的決定》都是规定互联网管理某一方面问题的单行法律，其他的规定大多散见于其他法律之中。应当我国现有的互联网法律、行政法规、部门规章进行梳理，同时借鉴境外经验，制定一部互联网管理综合性基本法律。

#### 2. 完善相关犯罪

现行的有关互联网犯罪的规定存在以下不足：第一，第 285 条第 1 款规定的非法侵入计算机系统罪的犯罪对象过窄，仅限于国家事务、国防建设和尖端科学技术领域的计算机信息系统三类。目前我国各行各业大都已建立自己的计算机信息系统，往往都事关经济建设和社会稳定，应当将非法侵入金融等重要计算机信息系统的行为纳入该罪。第二，规定单位犯罪。目前《刑法》第 285 条和第 286 条所规定的四个计算机犯罪都是自然人犯罪，没有将单位规定为犯罪主体。在现实中，由单位实施的互联网犯罪行为日益增多，危害更大，应当对上述四个犯罪增设单位犯罪主体。第三，增加过失犯罪的规定。上述四个犯罪都是故意犯罪，实际上过失行为同样会对互联网的安全造成重大危害，应当适当增加过失犯罪的规定，例如增设过失损坏计算机信息系统罪。

## 结 论

随着互联网技术的深入发展和计算机等网络设备的普及运用，网络犯罪数量已呈现出大幅度增长的态势，各种网络违法犯罪活动的频繁出现，给国家安全、社会安全、个人人身和财产安全带来严重威胁并造成巨额损失，已成为困扰现代人生活的重大问题，引起了社会各界的广泛关注。2012 年诺顿网络安全报告（目前是全球规模最大的针对个人用户进行的网络安全研究报告之一）的数据统计显示，过去的一年中，中国有超过 2.57 亿人成为网络犯罪的受害者，每天

有超过 70 万名中国网民遭受网络犯罪的侵害，平均每分钟就有 489 名受害者；而由于网络犯罪所造成的直接经济损失则达到 2890 亿元人民币，平均每位受害者蒙受的直接经济损失为 1126 元人民币。<sup>①</sup>

2012 年中国互联网违法犯罪最突出的三类问题凸显三大特征：一是以袭击网站和在线传播计算机病毒为代表形式的非法侵入和破坏计算机信息系统犯罪，其特征是高科技、隐蔽性。二是以攻击计算机终端用户实施的各种违法犯罪（如网络金融诈骗、网络盗窃、网络贪污、挪用公款、网络窃取国家秘密、网络侵犯商业秘密、网络刺探、泄露国家机密等），其特征是这些违法犯罪数量飞速增长、手段日益复杂化、侵害目的以获取经济利益为目的且数额巨大。三是通过网络平台实施的违法犯罪（如电子讹诈、网上走私、网上非法交易、电子色情服务、虚假广告、网上洗钱、在线侮辱、毁谤、网上组织邪教活动等），其特征是违法犯罪技术难度低，实施操作简便容易，社会影响范围广泛，已经称为中国网络违法犯罪的主要现象。根据公安部统计，在全国公安机关查处的众多网络违法犯罪案件中，网络赌博案、网络传播淫秽物品案、网络诈骗案、网络制贩假证假票案、网络传播贩卖大学女生被偷拍视频案、“浮云木马”网银盗窃案、非法获取计算机信息系统数据案、攻击敲诈香港金融业网站案

<sup>①</sup> 专栏与安全：“中国网络犯罪损失达 2890 亿”，2012 年 10 月。[www.pcworld.com.cn](http://www.pcworld.com.cn)。

等案件是 2012 年我国互联网违法犯罪的典型类型，对人民群众的人身财产安全和社会稳定造成的影响具有显著的代表性。

简言之，2012 年中国互联网违法犯罪呈现出犯罪嫌疑人学历高层次、岁数低龄化、犯罪手段智能性、犯罪过程隐蔽性、犯罪动机多元化、侵害范围广泛性等鲜明特点。随着个人电脑和移动手机的普遍使用，我国网民数量的不断增加，未来一段时间我国互联网违法犯罪将延续传统网络犯罪依然高发、犯罪数量继续增长的态势。传统犯罪借助信息网络广泛渗透，网络诈骗、网络赌博、网络色情、网络实体安全和网络个人信息侵害等高发性违法犯罪形式依然占据网络违法犯罪的主体位置；通过网络实施的侵财获利和窃取机密为主要目的违法犯罪案件将会有所上升；网络扰乱行为愈演愈烈，且逐步暴力化，严重影响社会秩序安定。

面对信息化技术带来的日益复杂的网络新形势，我国相关管理部门必须清醒认识互联网违法犯罪的特点和趋势，从加强和完善网络安全立法、增加网络安全意识、宣传网络先进文化、提高服务运营商的道德素质、保证计算机安全技术的稳定和发展等方面着手，政府、企业、社会组织密切合作，相互配合，责任共担才能切实减少和避免网络违法犯罪的发生，给广大网民营造一个和谐、文明、安全的网络环境。

（2013 年 1 月 18 日完稿）