海淀区人民法院2007年-2016年审结网络犯罪案件情况调研报告

游涛　杨茜

根据中国互联网络信息中心（CNNIC）发布的第38次《中国互联网络发展状况统计报告》，截至到2016年6月，中国网民规模达到7.1亿，互联网普及率达到51.7%，超过半数中国人已经接入互联网，安全的网络环境对庞大的网民群体和网络社会至关重要。互联网犯罪对社会稳定、经济发展、个人隐私的威胁越发严重。

海淀区作为中国的“硅谷”，拥有众多互联网企业，互联网基础设施完善，高科技人才汇聚，互联网普及率高，但是网络犯罪案件的发生频率也相对较高，统计分析我院近十年审结的网络犯罪[1]，能为研究我国当下网路犯罪提供典型样本，为防范网络犯罪提供可借鉴经验。

一、网络犯罪的定义与种类

（一）网络犯罪的定义

根据新出台的《网络安全法》对网络的定义是由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的网络和系统。所谓网络犯罪，是指互联网

[1] 本文的研究样本是2007年至2016年12月海淀法院审结刑事案件。

在犯罪过程中起到重要作用的犯罪活动；网络信息在犯罪活动中被侵害或被利用，是构成网络犯罪的实质要件。因此，凡是犯罪活动针对互联网发生的，或完全是在互联网上完成的，或以互联网为中介完成的，或利用了互联网资源的等等，都被作为网络犯罪纳入到本文考察的视野。

（二）网络犯罪的种类

网络犯罪都包括哪些具体种类？即网络犯罪的外延范围如何？本文重点在于研究网络犯罪的现状、审理难点和对策，因此依照犯罪学对犯罪类型的分类方法对网络犯罪类型进行划分，是可行的，也是必要的。犯罪学一般从犯罪行为特征、行为对象特征、行为人特征、行为人动机特征等对犯罪行为进行分类。笔者以此分类方法为标准，在吸纳其他官方或学者的观点的基础上，根据互联网在网络犯罪中所扮演的角色不同，归纳我院历年来审结的网络犯罪案件，将网络犯罪大体分为下列五个类别：一是破坏网络信息系统的犯罪，二是侵害网络信息数据的犯罪，三是以网络作为犯罪场所的犯罪，四是网络被作为中介利用的犯罪，五是利用网络资源进行的犯罪。

二、 海淀区法院审结的网络犯罪的总体概况及特点

2007 年至 2016 年间我国互联网基础设施建设和网络普及大幅提升，网络犯罪也日渐增多，这期间我院审结的网络犯罪案件呈现出总体态势增长平稳，近两年又日渐增多，涉案罪名种类繁多，网络诈骗及相关案件占比重，女性犯罪人比例高于普通犯罪，中青年高学历犯罪人比例高，犯罪呈现跨地域性，犯罪人户籍为京冀地区人数多的特点。2007 年至 2016 年本院审结的网络犯罪案件共计 322 件，其中

破坏网络信息系统的犯罪共计65件,侵害网络信息的犯罪共计27件,以网络作为犯罪场所的犯罪共计55件，网络被作为中介利用的犯罪共计123件，利用网络资源进行的犯罪共计52件。

（一）总体态势增长平稳，近两年却稳中有升

本院近十年审结的网络犯罪案件总体数量并不多，在近十年的全部审结刑事案件中占比也并不高，但是相较2006年之前的八年审判情况,网络犯罪案件数量已经出现明显增长的态势。1999年到2006年的八年间本院审结网络犯罪案件总计115件，占审结案件总数的5.84‰。而从2007年到2016年六月份，本院审结网络犯罪案件322件，占审结案件总数8.6‰。其发展变化如图1所示。尤其是2009年以后，各年网络犯罪数量虽然略有波动，不过始终维持在较高的数值，2009年至2014年这六年间本院年均审结网络犯罪案件34.8件，但是自2015年又出现大幅度增长。

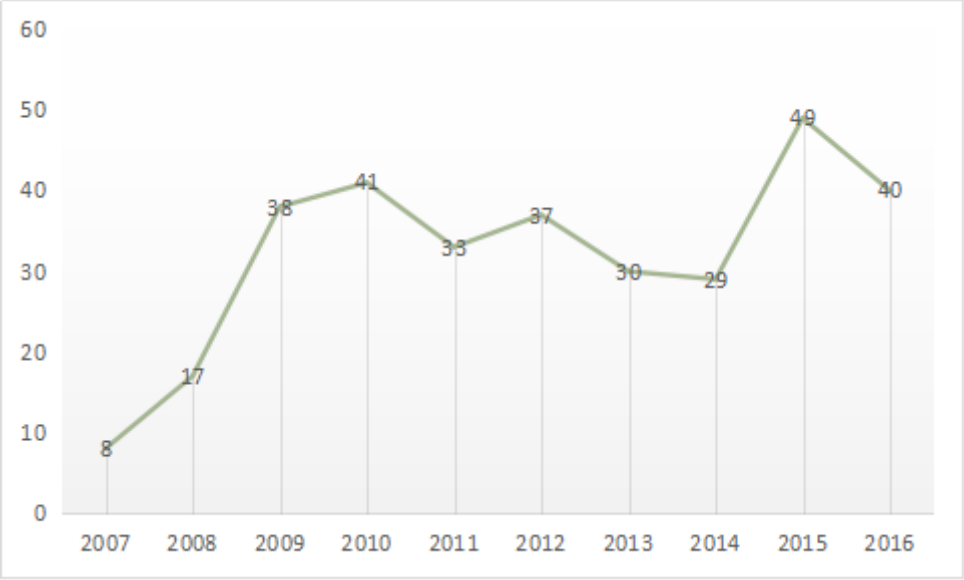

图1 本院近十年审结网络犯罪案件数量图

（二）涉案罪名种类繁多、网络诈骗及相关案件占比重

近十年网络犯罪涉案罪名剧增种类繁多，传统犯罪通过网络进行的日渐多发，高发案件类型和十年前相比，稍有变化，尤其是网络诈骗及其相关的犯罪明显增加，占比较重。

1、网络犯罪涉案罪名增多。在 1998 年至 2006 年期间，网络犯罪涉案罪名仅仅有 20 个罪名，主要集中于两个罪名，其一是利用邪教组织破坏法律实施罪，占网络犯罪总数 21.7%，其二是盗窃罪，占网络犯罪总数 22.6%。而从 2007 年至今网络犯罪涉案罪名已达到 47 个罪名（如图 2 所示）。与 2006 年之前的网络犯罪相比较，涉及罪名种类明显增加，主要是利用网络作为中介的犯罪和利用网络作为犯罪场所的犯罪明显增多，其中包含非法买卖枪支、伪造金融票证、销售有毒有害食品、出售非法制作的发票等传统犯罪类型。近十年以来，随着互联网、移动网和广播电视网的融合，网络从单一的信息传输平台变成为生活、服务的平台。网络的虚拟空间与现实社会更加复杂地交织在一起，这也为传统犯罪网络化提供捷径。

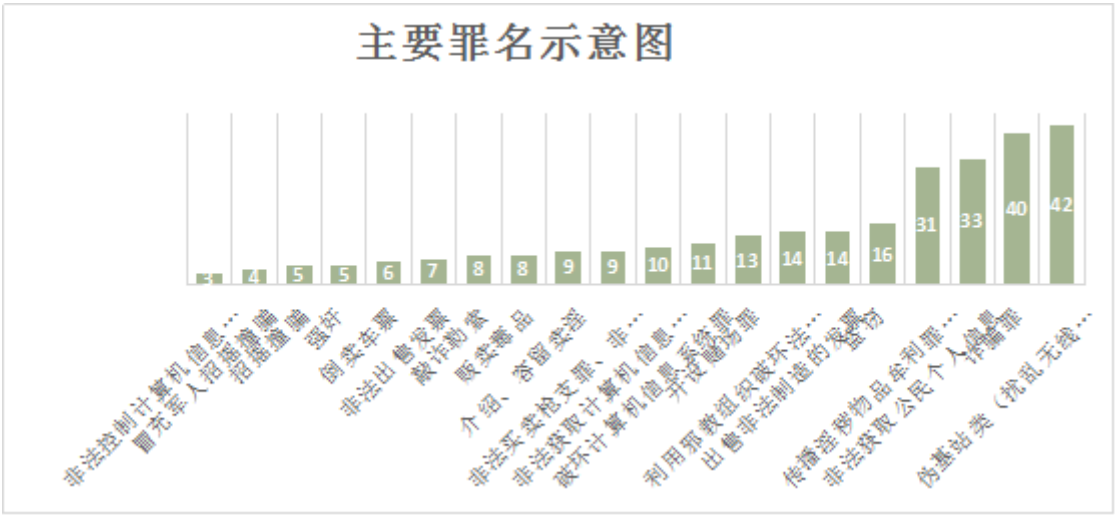

图 2 本院审结网络犯罪罪名与案件数示意图

2、网络诈骗及其相关犯罪占比重。2006 年之前网络犯罪案件中涉案罪名最多的是利用邪教组织破坏法律实施罪和盗窃罪。2007 年以来网络诈骗及其相关犯罪已然占据网络犯罪案件的突出位置，网络诈骗及其相关犯罪占比接近 40%。自 2007 年到 2016 年间，网络犯罪案件中涉案数量最多的是诈骗类犯罪，包括诈骗罪、冒充军人招摇撞骗罪、招摇撞骗罪、合同诈骗罪，共计 52 件，占据网络犯罪总数的 16.1%，其次是伪基站犯罪，共计 42 件，占网络犯罪总数的 13%，再次是非法获取公民个人信息罪，共计 33 件，占网络犯罪总数的 10.2%。多数获取公民个人信息、利用伪基站群发短信的案件也是为网络诈骗做准备，所以近十年以来网络诈骗及其相关犯罪成为最为常见的网络犯罪。此外，传播淫秽物品类犯罪、盗窃罪、利用邪教组织破坏法律实施罪的案件数量依旧位于网络犯罪案件的前列(详见图 3)。此外，网络诽谤和侮辱行为也呈爆发态势，本院立案受理的刑事自诉案件近八成为网络诽谤，然而由于刑事案件入罪标准和证据审查的严格，这些案件往往由于证据不足被驳回起诉或者达成和解。

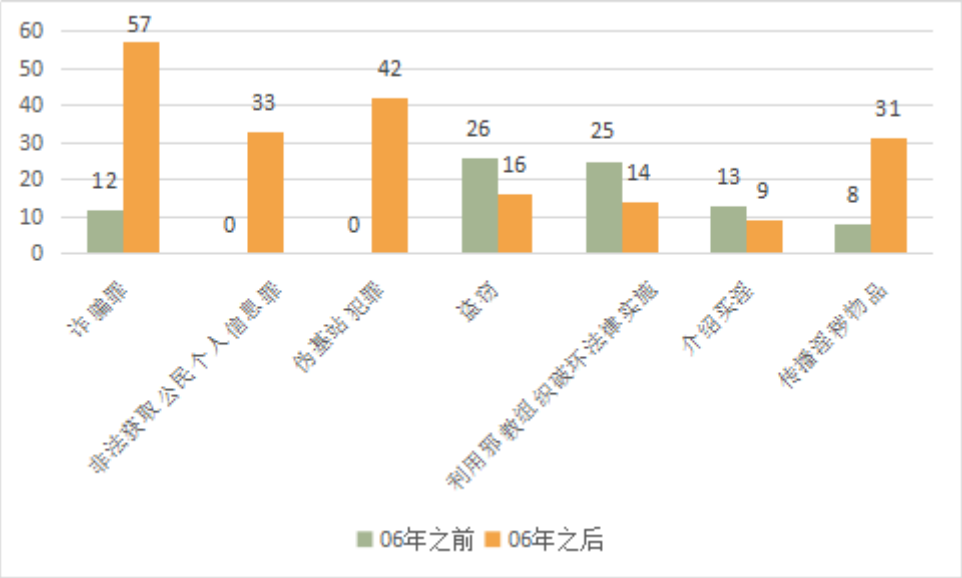

图 3 2006 年前和近十年网络犯罪主要罪名变化对比图

（三）女性犯罪比例高，高学历青年为主

1、女性犯罪人比例高于普通犯罪。在 2006 年之前的网络犯罪中，在 189 名网络犯罪人中，女性 53 人，占总人数的 28.04%，女性犯罪人占比远高于其他犯罪。而近十年来的网络犯罪中，在 450 名罪犯中，有 82 名女性，占 18.2%，依旧远高于其他类型犯罪，普通犯罪中女性占比仅仅接近 15%。然而和 2006 年之前的网络犯罪人相对比，女性犯罪人数比例有所下降（详见图 4）。不过，在一些犯罪中，男性犯罪人比例占据绝对多数，例如本院审结的 31 件传播淫秽物品和 10 件非法持有枪支、非法买卖枪支案件中，犯罪人全部为男性。

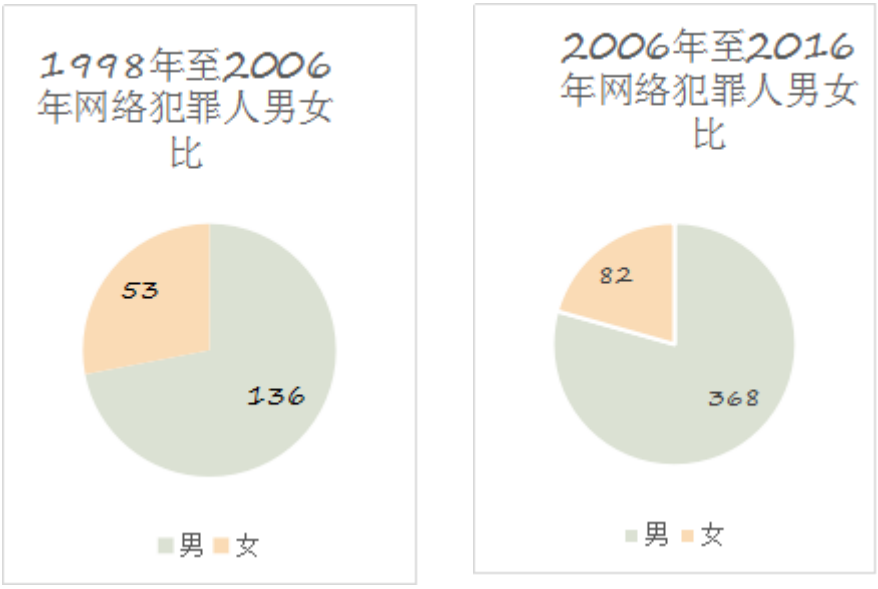

图 4 网络犯罪人男女比

2、网络犯罪中犯罪人多为青年。网络犯罪人年龄分布集中在 20 岁到 40 岁青壮年，这也符合我国网民年龄分布。根据 2015 年互联网发展状况报告，我国 20 到 39 岁网名占 54%。而网络犯罪中 20 岁到 39 岁的占了 85.9%，成为网络犯罪的主体。在破坏网络系统的犯罪和侵害网络信息的犯罪中，犯罪分子几乎全部在 40 岁以下。这两个类型的犯罪对网络技术水平要求比较高，青年人使用互联网的熟练程度和计算机技能远胜于中老年人，成为犯罪主要人群也是情理之中，而 40 岁以上的犯罪人主要集中在其他三个类型犯罪，这三个类型犯罪和传统犯罪紧密相关，对网络技术要求较低。与 2006 之前的网络犯罪人的年龄相对比，近十年来网络犯罪人低龄化的趋势十分突出，20 岁至 40 岁的青年人成为本类型犯罪主力（详见图 5）。

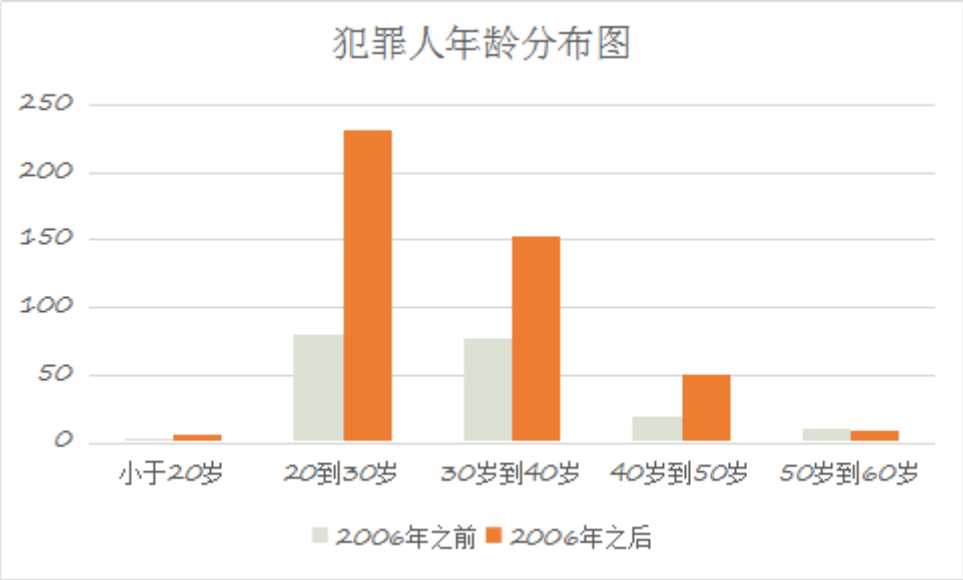

图 5 本院审结网络犯罪年龄分布图

3、高学历犯罪人占比较高。在全部犯罪人中，大专以上学历的罪犯占网络犯罪全部犯罪人数的 45%。而同期我院审结案件中近 72%的的犯罪人学历在初中以下。2006 年之前的网络犯罪，大专以上学历犯罪人仅仅占 39.8%，而近十年网络犯罪中大专以上学历犯罪人的占比已攀升至 55.3%（详见图 6）。而且网络的快速发展，庞大的网民基数和多点上网的方式为网络犯罪提供了新的犯罪契机，一个犯罪人可以通过提供技术、程序、软件等传授给没有相关计算机技术和技术的犯罪人实施犯罪行为，这也使得网络犯罪像“病毒”一样极易扩散。所以在网络犯罪中低学历人群数量不断增加。

图 6 本院审结网络犯罪的学历分布情况

4、罪犯地域分布广，京冀罪犯最常见。在本院审结的案子中，河北、北京犯罪人占比最高，河南，山东等人口大省占比也不低（详见图 7）。由于网络的联通性，跨地域犯罪十分常见，犯罪行为预备地、实行地和结果地往往不在同一地域，例如本院审结的利用网络开设赌场罪中犯罪人 71%为北京人，在本辖区利用网络为境外赌博组织做代理，参与赌博者则遍布全国各地。此外，由于三网融合，人与系统的互动和人与人的互动越发疏散，不在受制于地域限制，使得在网络空间中进一步相互配合而实施共同犯罪的现象大量出现。

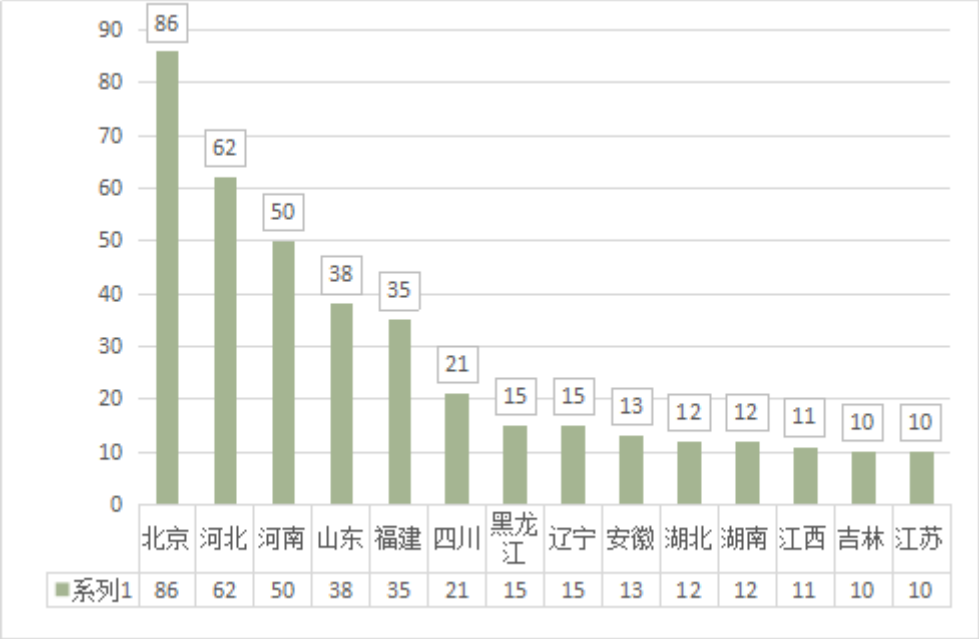

图 7 本院审结的网络犯罪人区域分布图

三、五大类型网络犯罪的现状及特点

根据前文笔者将网络犯罪分为五大类型，下面将就这五种类型的网络犯罪一一分析现状及特点。

（一）破坏网络信息系统的犯罪

破坏网络信息系统的犯罪是针对网络系统实施破坏措施的行为，其行为核心特征是破坏行为。和 2006 年以前相对比，本院审结的此类型犯罪呈现出明显变化，有如下特点：

1．涉案罪名增多，案件数量剧增。2006 年以前破坏网络信息系统的犯罪仅有 1 件，近十年本院审结此类案件增多至 65 起，涉案罪名也增加 7 种；

2．作案手段技术化，犯罪规模产业化。由于犯罪技术如黑客技术、病毒研发技术越发成熟，相关犯罪设备如“伪基站”更加容易

获得，一个犯罪人可以迅速将犯罪手段教给其他犯罪人，规模化现象明显；

3．诈骗案件增长快，上下游犯罪惊人。网络诈骗催生上下游犯罪产业链，以网络诈骗为核心，盗取公民个人信息和电信诈骗类案件急剧增长，近十年本院审结的网络诈骗及其相关案件高达 127 起（详见图 8）。

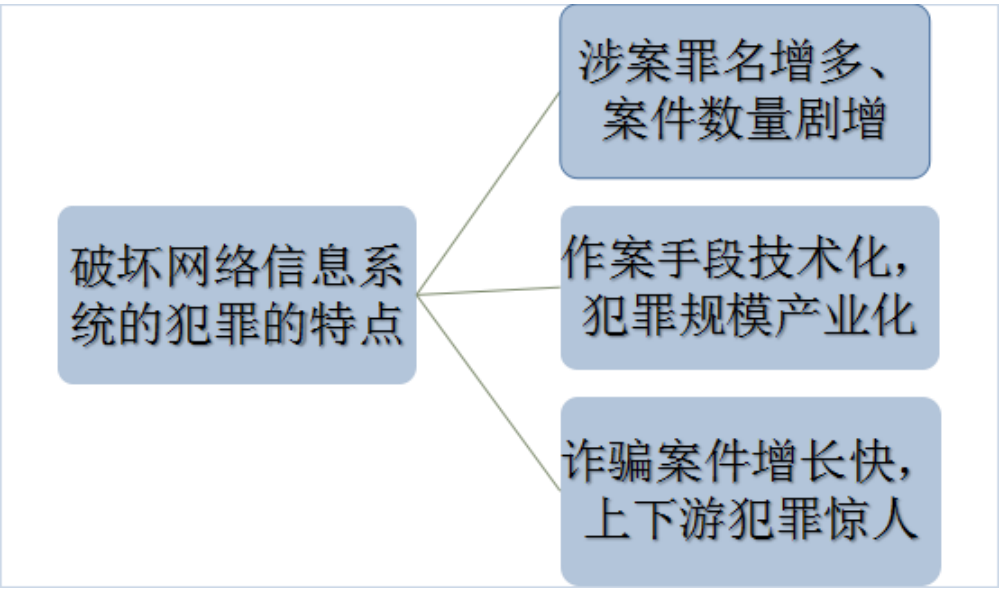

图 8 破坏网络信息系统的犯罪特点示意图

根据破坏计算机信息系统是目的还是手段分类，此类犯罪又可以分为两种：

1．破坏网络作为犯罪目的，即将计算机信息系统作为犯罪对象进行破坏，包括破坏计算机信息系统罪、扰乱无线电通讯管理秩序罪、破坏公用电信设施罪和非法控制计算机信息系统罪；

2.破坏网络作为犯罪手段，即将破坏计算机信息系统作为前行行为和犯罪手段，以实施传统犯罪，破坏网络是犯罪的必需手段，而

非目的。包括通过破坏计算机系统实施盗窃、诈骗、敲诈勒索的犯罪。本院审结侵害网络系统的犯罪中案件数量最多的是“伪基站”类犯罪，共计 42 件。其次是破坏计算机信息系统罪，共计 11 件（详见图 9）。

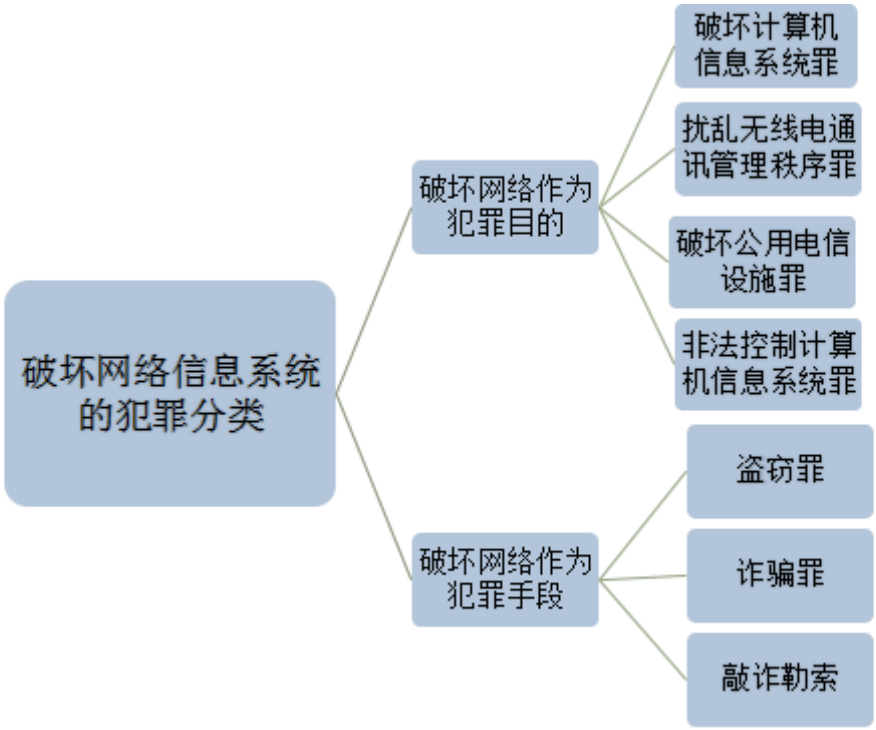

图 9 破坏网络信息系统的犯罪的分类示意图

以破坏为目的的犯罪中，“伪基站”犯罪是最多发的犯罪类型，本院审结的这 42 件案子都是利用伪基站发送诈骗消息和推销广告。其特点有：

（1）流动性作案。犯罪人多是将“伪基站”设备放置在汽车中，汽车缓慢行驶或者在商场、车站等人流密集区域，进行短信发送；

(2)学历低男性化。本院审结的“伪基站”类犯罪人中 77.7%的人只有初中以下学历，除了两名女性罪犯，93%的犯罪人为男性，而且犯罪人全部为 20 至 40 岁的青壮年；

(3)诈骗相关性。这类垃圾短信往往包含诈骗信息，关联钓鱼网站，为网络诈骗埋下接入口。

破坏计算机信息系统罪则是最为典型的网络犯罪。本院审结的这11个案子,有以下特点：

(1)学历高有职业。犯罪者具有学历水平高、青年男性为主、有正当职业者较多的特点，23名犯罪人，21名具有高中以上学历，以男性为主，女性仅占26%，公司高管等有正当职业者有10人，平均年龄29.3岁；

(2)作案技术性强。包括删除、修改信息数据，制作、传播破坏性程序，利用僵尸网络进行流量攻击、信息窃取、发送垃圾邮件、监听流量等恶意网络行为。这11起案件中只有两起案件是内部人员通过卸载杀毒软件或者删除源代码导致系统瘫痪。这些案件成为典型的黑客入侵案件，一方面给受害方造成财产损失，另一方面也为网络安全敲响警钟。例如，2015本院审结的一起破环计算机信息系统罪中案件被告人蒋某身为公司首席技术官,因为和公司法定代表人之间的待遇纠纷，擅自删除、下载公司正用于软件产品开发的计算机源代码等文件，导致公司产品开发进程受阻，产生严重损失。

非法控制计算机信息系统罪是对计算机信息系统进行破坏继而实现控制的行为，这类犯罪也为实现其他犯罪提供“桥梁”和“敲门砖”。近十年来本院审结的总计三件，数量上并不多。该类案件行为

上有两种方式：一是利用技术手段侵入电脑形成僵尸网络；二是利用“撞库”获取用户信息进行牟利。

此类犯罪行为人侵入计算机信息系统后，控制计算机进行其他活动，以2015海刑初2447号所判决的案件为例，张某利用其租用的VPS服务器作为主控服务器，在使用自己的电脑登陆服务器后，利用SYN扫描器扫描出互联网内存在WDCP漏洞的计算机信息系统，并使用“Mysql.exe”文件取得上述计算机信息系统的控制权，随后利用其租用的VPS服务器内“3600集训”软件生成名为“ip32.rar”的木马文件，再利用SSH连接器将该木马上传至其控制的计算机信息系统上，致使该计算机信息系统对外做DDOS流量攻击。这个案件反映出当下木马产业链的冰山一角，目前僵尸网络的出租已经形成规模，很多网络犯罪都需要通过僵尸网络进行后续犯罪，而僵尸网络的建立，只有一个目的就——钱；建立僵尸网络后可以通过DDOS攻击、窃取机密信息、发送垃圾邮件、钓鱼网络诈骗、广告点击诈骗以及传播恶意软件和广告软件来获得利益，这也导致非法控制计算机的犯罪日益增多。

值得注意的是，本院在2011年审结过一起提供侵入、非法控制计算机信息系统的程序、工具罪案件，这起案件也是审结案件中唯一涉及此罪名的案件，被告人经营网站期间，为吸引收费会员、增加网站盈利，由员工向VIP会员区及相关版块上传大量专门用于侵入、非法控制计算机信息系统的程序、工具及相关技术教程供会员下载。这

种行为虽然没有直接造成网络系统的损害，但是因为提供了犯罪的工具且该帮助行为已被刑法分则的相关规定予以正犯化，因此上述帮助行为依旧成立犯罪正犯行为。这个案例中也反映出近年来网络犯罪的一个特点，黑客技术手段越发成熟，传播教授犯罪手段和工具越发容易，黑客的进入门槛由于这些帮助行为一再降低。

（二）侵害网络信息数据的犯罪

侵害网络信息犯罪行为是指非法侵入网络，并不破坏互联网系统，获取的往往只是时间、权限、数据等网络信息，但却给他人造成了现实的资费、财产的损害。与 2006 年之前相比较，该类犯罪的变化并不明显，其特点有：

1.案件数量相对较少。1998 年到 2006 年本院审结此类案件数是 26 起，近十年本院审结此类案件数是 27 起，数量持平，相较于其他四种类型的网络犯罪吗，案件数量最低；

2.学历高男性化。与 2006 年之前此类犯罪相比较，犯罪人依旧以青壮年男性为主，女性犯罪人比例持续下降，32 名犯罪人只有 2 名女性，女性仅占 6.25%，而在 2006 年之前，此类犯罪的女性犯罪人占比 13.8%，犯罪人学历较高，高学历犯罪趋势加强，近十年此类犯罪人 51%为大专以上学历，而 2006 年之前大专以上学历的犯罪人不足 45%；

3.犯罪手段无翻新。与 2006 年之前的侵害网络信息数据的犯罪相比较，近十年此类犯罪行为上具有相似性，犯罪手段并没有翻出新

花样，这类犯罪虽然没有破坏计算机信息系统，但却合法或者非法进入信息系统，造成实际的财产损失或者数据泄露。常见的行为方式包括：①合法手段进入网络信息系统，如内部员工利用职务便利，进入公司系统侵占或盗窃财物；②非法手段侵入信息系统，主要有冒充合法用户侵入网络信息系统，如盗窃、非法获取真实用户信息进入信息系统，或者利用技术攻击手段突破网络安全防卫机制、或者通过系统漏洞或 “后门”进行非法入侵（详见图 10）。

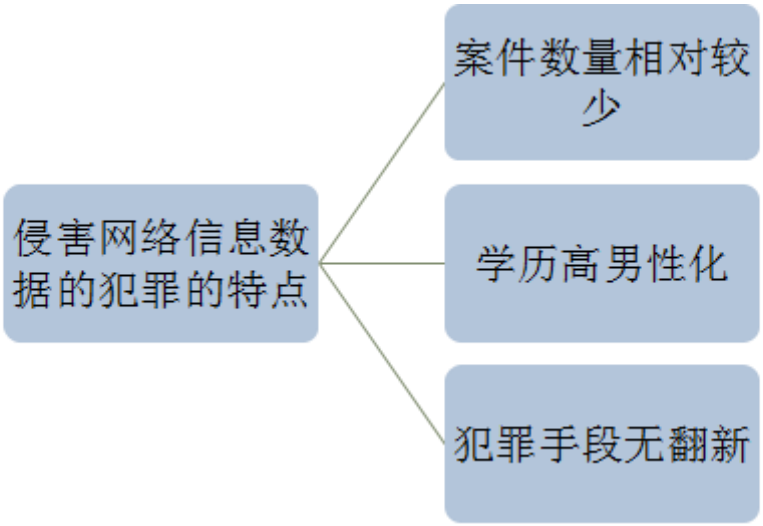

图 10 侵害网络信息数据的犯罪的特点示意图

以侵犯的犯罪客体为依据，此类犯罪可以分两类：

1. 侵害财产权益的犯罪，其中包括盗窃罪、职务侵占罪、诈骗罪、侵犯商业秘密罪和敲诈勒索罪，这类犯罪以非法方式比如植入木马、利用漏洞、盗取账户、利用职务便利非法进入信息系统等，通过更改信息等方式以直接获得实际的财产利益；

2. 侵害计算机安全的犯罪，包括非法获取计算机信息系统数据罪，这种犯罪也通过非法的方式进入信息系统，获取信息数据，比如虚拟

财产等信息数据，对财产权益的侵害是间接的，主要侵害的是信息系统的安全。

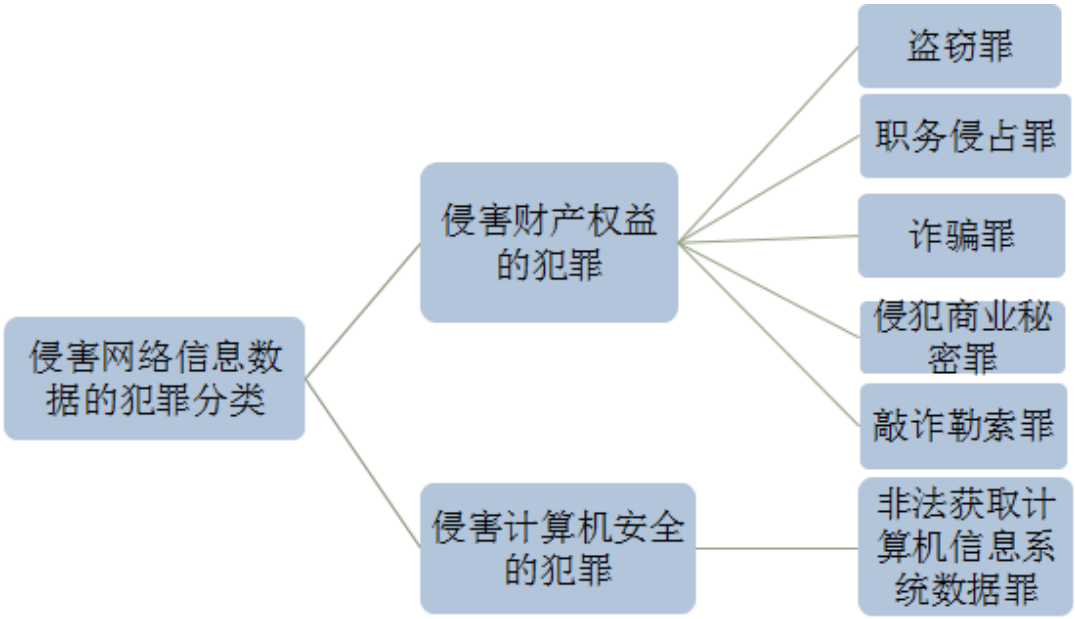

图 11 侵害网络信息数据的犯罪分类示意图

侵害网络信息犯罪中有 17 件直接侵害财产权益的案件，其中盗窃罪案件数最高，共计 14 件。**利用侵入网络信息系统获利的这一类具有如下特征：**

（1）身份职务化、手段技术化。15 名犯罪嫌疑人中 8 人供职于网络公司，而职务侵占罪案件中 3 名犯罪人全部是公司职员，这类非法获利的犯罪行为不同于传统盗窃罪等侵犯财产的犯罪，具有高难度、高技术的特征，需要利用职务便利或者专业化的网络技术进行犯罪行为，这就要求犯罪人具有进入网络信息系统的权限，如公司财务人员等，或者拥有相关技术知识，这种“键盘一敲，财源滚滚”的行为与传统的扒窃、入室盗窃等行为有很大区别；

（2）犯罪所得巨大。传统盗窃手段的非法所得很难和网络犯罪的涉案金额相比，网络犯罪中利用侵入信息系统，通过转账或者技术盗窃的手段，获利往往惊人，近十年本院审结网络盗窃平均每个案件犯罪所得高达635363元，例如2015年本院审结的一起中石油员工盗窃案[2]中，拥有硕士学历顾某多次使用私自编写的程序，对其事先购买的上千张中国石油昆仑加油卡进行非法充值，后又倒卖上述加油卡牟利，非法充值数额共计人民币700余万元，给中国石油天然气集团公司造成严重经济损失。这个典型的网络盗窃案例深刻体现出网络犯罪职务化、高科技化、危害巨大的特点。目前在审判实践中将获取实际财产的行为认定为盗窃行为，并未将非法获取虚拟财物纳入此类犯罪中。

侵害计算机网络安全的犯罪，非法获取计算机信息系统数据罪是最为典型的犯罪。近十年以来本院共审结此类犯罪案件9件，这类行为突出特点是：

（1）学历高年纪轻，犯罪人中43.5%具有大专以上学历，全部为青年男性，平均年龄27.28岁；

（2）费尽心机获取信息，该类犯罪行为上表现为对网络数据的非法获取，典型犯罪模式有两种：①利用漏洞或者盗取性软件获取网络信息，如账户名称密码、游戏币等，并将此类信息贩卖，这种尤其常见于盗取游戏系统的信息的案件，本院审结的9件此类案件有8件

[2] 参见（2015）海刑初字第1323号刑事判决书。

是盗取游戏账户号和游戏币的案件；②非法进入数据库获取用户信息。非法获取计算机信息系统数据的行为与破坏网络系统的犯罪最大的不同是，没有对网络系统进行破坏，而仅仅是对数据进行非法复制。

（三）以网络作为犯罪场所的犯罪

该类犯罪将网络作为犯罪的平台，作为实施犯罪的“主阵地”，并不破坏网络系统或者侵害网络信息，而是在互联网上完成所有的犯罪行为便达到了犯罪目的，或在互联网上完成主要的犯罪行为，再辅之现实世界的一些手段行为，即达到了犯罪目的。笔者将此类既侵犯网络信息，又实际占有他人财产或完全实现犯罪目的之犯罪类型，归纳为以互联网作为犯罪场所的网络犯罪。近十年本院审理的这类犯罪共有 55 件，与 2006 年之前的此类犯罪相比较，其特点是：

1.案件数量翻倍，涉案罪名翻新。2006 年之前的八年间本院审结此类犯罪共 35 件，而近十年本院审结此类案件 55 件，增长近 1 倍。犯罪罪名涉及掩饰隐瞒犯罪所得罪、敲诈勒索罪、销售有毒有害食品罪、侮辱罪、诽谤罪、敲诈勒索罪、开设赌场罪、过失或故意泄漏国家秘密罪、传播淫秽物品罪和传播淫秽物品牟利罪等。这些犯罪行为侵害的法益相当广泛，既有侵害社会秩序的案件也有侵害人身健康和财产安全的案件；

2.犯罪手段花样多。相较于 2006 年之前的此类犯罪，近十年间此类行为犯罪既有利用网络发布信息编造谣言、恶意中伤、散布隐私的侮辱诽谤行为，还有通过网络发布虚假消息恐吓他人的敲诈勒索，

最为常见的是开设赌博网站或者为设在境外的赌博网站做代理进行非法赌博的行为，以及在网站或者微博博客上公开散播淫秽物品的行为；

3.学历高男性多。74 名犯罪人中学历水平较高，以青年为主，此类犯罪人平均年龄 33 岁，共计 70 名男性和 4 名女性，女性占比较低，以男性为主。其中传播淫秽物品和传播淫秽物品牟利罪的罪犯全部是男性。而学历水平较破坏网络信息系统的犯罪和侵害网络信息数据的犯罪，学历普遍较高，高中以上文化水平的犯罪人占 72.9%（详见图 12）。

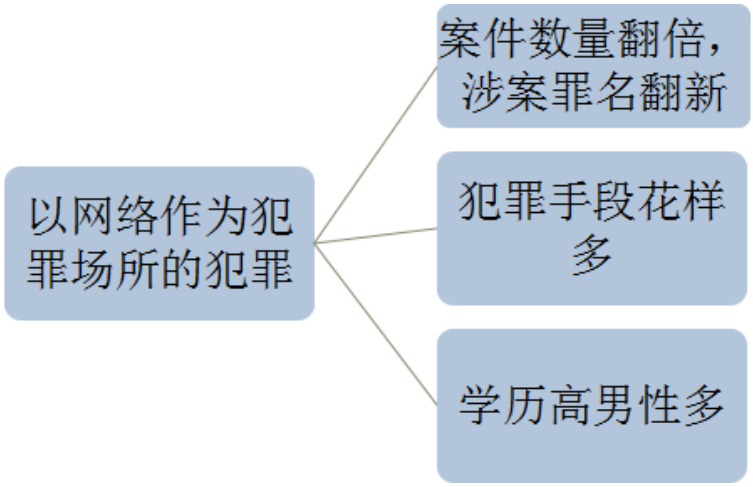

图 12 以网络作为犯罪场所的犯罪分类示意图

按照侵害权益的不同，该类犯罪又可以分为：

1.侵害公民财产权益的行为，包括利用网络进行敲诈勒索

2.侵害公民名誉的行为，包括侮辱、诽谤；

3.侵害社会正常秩序的行为，包括掩饰隐瞒犯罪所得罪、售有毒有害食品罪、开设赌场罪、过失或故意泄漏国家秘密罪、传播淫秽物品罪和传播淫秽物品牟利罪等（详见图 13）。

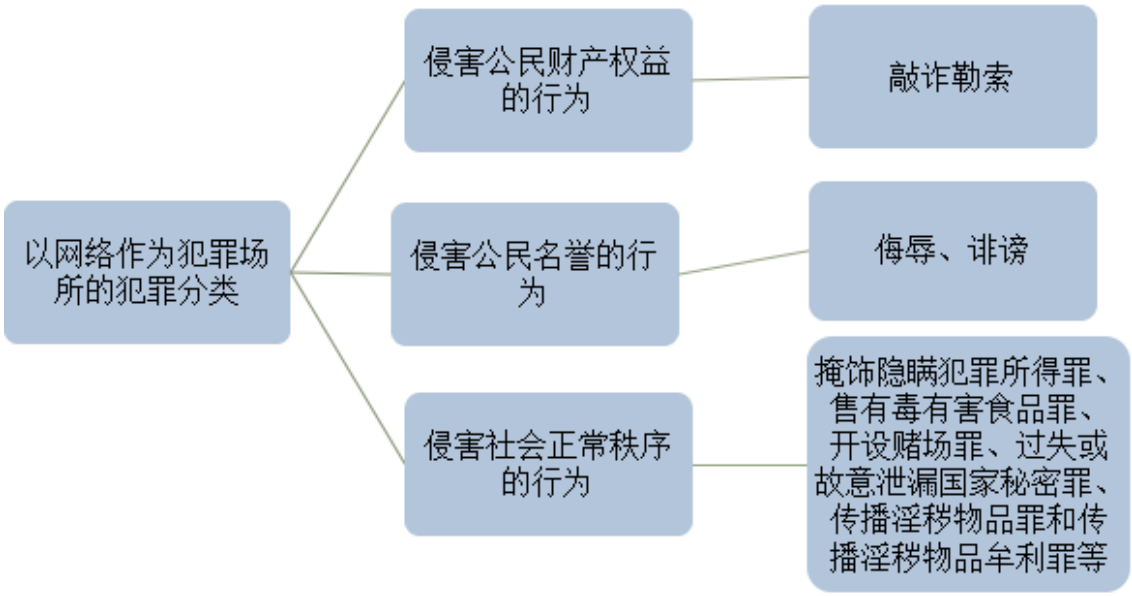

图 13 以互联网作为犯罪场所的犯罪分类示意图

以互联网作为犯罪场所侵害公民名誉的侮辱、诽谤罪目前本院共审结定罪 1 起。自 2013 年两高出台了《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》，根据该解释诽谤他人达到情节严重的可以追究刑事责任。不过刑法具有谦抑性，只有行为的社会危害性程度达到足够犯罪的程度才能追究刑责。本院近年来立案的侮辱、诽谤罪自诉案件一直呈现上升趋势，不乏一些社会热点案件，比如洪道德诉陈光武诽谤案，本案后来经过调解圆满解决。大部分网络诽谤自诉案件由于被调解或者定罪证据不充分被驳回，这也显示本院适用刑法的审慎。目前定罪的 1 起案件，被告人在各个网站上发布

自诉人的个人信息及照片，并恣意对自诉人进行诽谤、侮辱，还将自诉人及家人个人资料编造后在网络上发布，以“通缉”等字眼寻找自诉人，这种行为已经达到值得刑事处罚的程度才被定罪为侮辱、诽谤罪。

在以互联网作为犯罪场所的侵害社会秩序的案件中，以开设赌场罪和传播淫秽物品行为最为突出。近十年本院审结开设赌场罪案件13起，传播淫秽物品类犯罪案件31起，掩饰隐瞒犯罪所得案件2起，泄露国家秘密案件4起。**这类以互联网为犯罪场所的犯罪行为有以下特点：**

1.男性化，有业者居多。此类犯罪中男性犯罪人为主，北京户籍有较高文化程度有职业者居多。开设赌场罪的13名被告人中仅有1名女性，其中9名是北京户籍犯罪人，占比69.2%。传播淫秽物品的31件案件更是无1名女性犯罪人，男性犯罪人占比100%，其中21人有职业，占67.7%，职业涉及网吧经营者、网站编辑、医生、公司职员、教师等不同各业，包括一些互联网企业经营者和管理者。故意或者过失泄露国家秘密的案件中，4名犯罪人全部为男性，3人为北京户籍。64名犯罪人除去10人仅为初中或小学文化，其余全部具有高中以上学历，其中传播淫秽物品犯罪案件中64.7%的犯罪人具有大学以上学历，其中包括3名硕士学历犯罪人，泄露国家秘密的4件案件中，2名具有博士学历，2名具有大学学历，体现出网络犯罪者高学历的典型特点；

2.犯罪行为本地多，危害后果跨地域。13 件开设赌场罪案件中 12 件是犯罪人为境外赌博网站担任代理，在北京本地作案，为境外赌博网站招揽赌徒，这些赌博网站的参赌人员分布广泛，体现出跨国跨区域的特点。传播淫秽物品类犯罪的行为方式基本是互联网用户在本辖区内利用网站、博客、微博、论坛等公开传播淫秽图片、小说、视频。其中 2015 年审结的三起传播淫秽物品牟利罪的案件[3]具有典型性，这三起案件的犯罪人全部是新浪阅读频道的编辑和作者，这是本院第一次将合法经营网站的管理者作为传播淫秽物品类犯罪的犯罪主体追究刑责。 2016 年审结的快播案则是将网络企业和高管一起作为传播淫秽物品罪的犯罪主体予以追责。本案也是将网络监管义务从自我监管提升到法定义务的一个典型案例，对网络服务提供者的日常监管责任进一步明确。而互联网的开放性使得淫秽音视频和图片的点击率惊人，其扩散的速度、对青少年网民的危害不可估量。泄露国家秘密的行为方式则比较单一，行为人将国家秘密在网络上传播、或者违反安保规则处理涉密信息；

3.故意犯为主，偶有过失犯。本院审结的开设赌场罪和传播淫秽物品罪的犯罪人无论动机是牟利还是博取点击量，全部具有主观故意，以直接故意为主，也存在间接故意。如快播案中四名高管，作为网络信息服务提供者负有网络安全管理义务，明知其缓存服务器存储淫秽视频而放任存储、传播的行为具有间接故意。过失犯则体现在泄

[3] 参见（2015）海刑初字第 513 号刑事判决书、（2015）海刑初字第 821 号刑事判决书、（2015）海刑初字第 822 号刑事判决书。

露国家秘密的犯罪中，这其中有 2 件是过失泄露国家秘密，例如 2010 年本院审结的一起案件[4]，被告人董某作为中科院某研究室副主任，违反保密规定，多次在个人购买使用的笔记本电脑上存储、处理涉密信息，并连接互联网使用该电脑，致使该电脑被台湾间谍情报机构远程控制，并从该电脑上窃取 3161 份文件资料。经鉴定，被窃取的材料中属于机密级国家秘密 8 份、秘密级国家机密 15 份。董某被认定为过失泄漏国家秘密罪。互联网自身的安全性存在隐患，极易被操纵和远程控制，泄漏秘密和机密，这就需要有关人员必须严格执行保密规范。

（四）网络被作为中介利用的犯罪

此类犯罪系利用互联网作为信息媒介和中介，主要犯罪行为发生在现实世界，换言之互联网在这类犯罪中主要起到中介的辅助作用，具体的犯罪行为都在现实世界发生，并不依赖网络。本院近十年审结此类案件共计 123 件。相较于 2006 年之前的网络犯罪，这类案件呈现出如下特点：

1.数量井喷、罪名集中。案件数量呈现井喷式增长，涉及罪名以诈骗、介绍买淫和买卖违禁物为主。2006 年之前的八年本院审结此类案件数仅有 33 件，而 2006 年之后的近十年间本院审结此类案件 123 件，呈现井喷式增长；

[4]参见（2010）海刑初字第 4061 号刑事判决书

2.学历低多无业。与2006年之前的犯罪人近似，近十年此类犯罪的犯罪人依旧表现出低学历、低收入的特点。190名犯罪人中，女性有56名，占29.4%，远高于其他类型的网络犯罪。190名犯罪人中119人只有初中以下学历，高中以上学历仅占37.7%。有91人无职业，占比近47.3%；

3.作案手段技术含量低。在智能手机普及之后，微信等社交软件和各类电商兴起，利用互联网作为沟通媒介已然最基本的生活技能，相伴而生的是用网络做信息媒介实施传统犯罪的案件陡然增多（详见图14）。

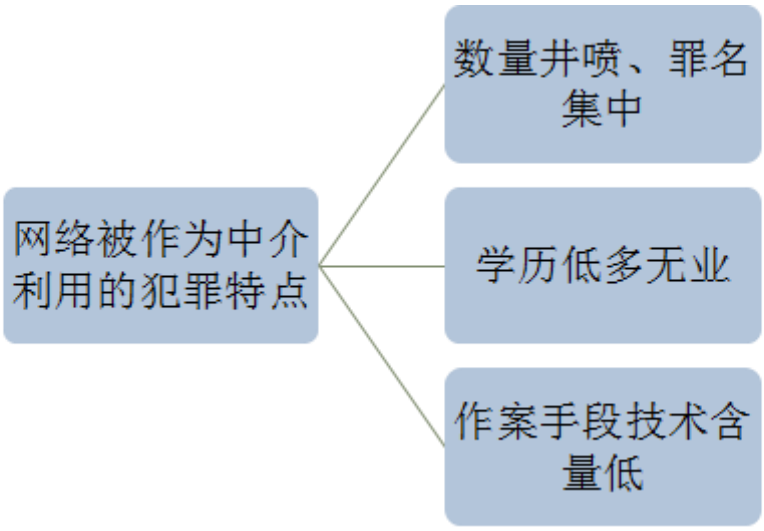

图14 网络被作为中介利用的犯罪特点示意图

利用网络作为中介的网络犯罪按照犯罪侵害的法益是公民财物还是社会秩序的不同，分为两类：

1.诈骗类，涉案罪名包括诈骗、招摇撞骗、合同诈骗、冒充军人招摇撞骗等；

2.非法买卖类，包括非法持有枪支、贩卖毒品、出售非法制造的发票、倒卖车票之类的买卖违禁品犯罪和介绍卖淫犯罪（详见图 15）。

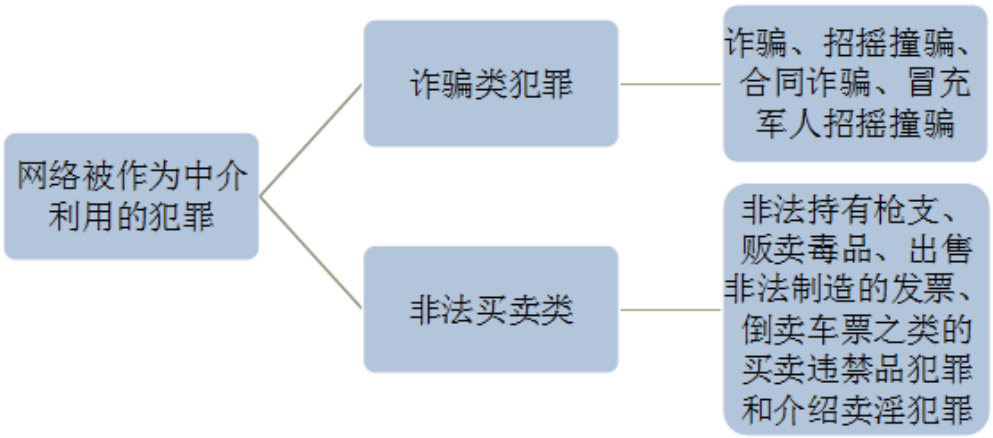

图 15 网络被作为中介利用的犯罪的分类示意图

网络被作为中介利用的诈骗类犯罪，包含诈骗罪，敲诈勒索罪，招摇撞骗罪，冒充军人招摇撞骗罪，合同诈骗罪，如果将网友欺诈约会的强奸犯罪也计入该类罪名，共计有 52 件。**这类诈骗行为有以下特点：**

（1）数量惊人，这类案件占据网络犯罪总数的 16.1%，是数量最多的一类案件。

(2)网络交友骗子多，网购骗局陷阱深。这其中有 27 件利用网络交友骗取网友钱财，手段均是通过 QQ、微信、婚恋网站等社交软件或者平台，虚构如警察、军人、富商等的身份，取得网友信任，进而骗取钱财，甚至在实际见面时实施强奸、抢劫，本院审结的网友会面实施强奸的案件有近 10 起，这类诈骗案件受害者绝大多数是女性，

仅有一起案件被害人是男性，男性作案者通过虚构自己女大学生的身份骗取这名被害人的钱财，手段令人唏嘘。这类案件也说明通过虚拟网络交友风险极高，尤其是女性本性善良软弱，极易轻信陌生人，因此女性网民更需要加强防范。另一种则是网购骗局，本院审结 18 起此类诈骗案件，这种诈骗往往发布虚假信息，通常是低价购物诱使消费者上当。例如发布虚假购电影卡信息，号称自己是电影公司内部员工，给出优惠价吸引消费者，或者发布虚假团购信息，或者开设虚假淘宝网店代卖低价飞机票或者通过发布虚假高薪招聘信息、虚假学历培训信息和虚假评级评奖信息，获取信任诈骗钱财。有的犯罪人通过正规交易网站发布虚假打折商品信息以骗取消费者信任，有的通过开设虚假公司和网站，骗取会员财物，还有一些典型的网络诈骗行为，如利用弹窗发布虚假中奖信息，使用电话假扮客服等骗取财物。这也提示消费者和广大网民在上网时一定要提高警惕，对涉及财物交易和转账行为一定要考察清楚对方的资格。

例如，本院 2009 年审结的一起金某诈骗案[5]，该案中金某通过其管理的“东方神起”歌迷网站（www.tvxq.com.cn），向网民发布可以代买“东方神起”上海、北京演唱会门票及纪念产品的消息，要求有意购买的网民向其指定帐户汇款，先后骗取被害人 265 人，诈骗金额人民币 431 215.3 元。

[5] 参见（2009）海刑初字第 1143 号刑事判决书

网络被作为中介的违禁品买卖和介绍卖淫，也是在网络成为信息服务主要媒介之后，案件数量日渐增长。近十年间本院审结的介绍卖淫罪案件共计8件，非法持有枪支案件10件，贩卖毒品案件8件，倒卖车票案件6件，出售非法制造的发票案件14件。**这类犯罪有如下特点：**

(1)涉枪犯罪增长快、高学历人群成购枪主流。本院审结的10起非法持枪案件中，犯罪人通过网络论坛、微信等途径便可购买枪支，犯罪人均为大专以上学历的男性，有2名被告人有硕士学历。仅3名犯罪人无职业，其他犯罪人均有稳定职业，不乏工程师、公司职员、摄影师、大学教师等社会精英，这类犯罪的高学历水平与其他利用网络作为中介的犯罪极为不同，这类人群受到良好的教育，却触犯法律的底线，这也说明有法必依，否则就将受到法律惩罚。此外网络贩枪的猖獗也令人震惊，通过快递就能购买、运输枪支，这也提示监管方和网络平台需加强管控，切段网络贩枪的渠道。

(2)兜售假航空运输电子客票行程单成规模。近十年本院审结14起出售非法制造的发票案件，无一例外的在网上兜售假航空运输电子客票行程单。这一犯罪已然成为制售假发票犯罪的 “新宠”；

(3)社交平台涉黄赌，违法交易速达成。通过QQ群、朋友圈、陌陌等社交平台购买毒品和介绍买淫成为新趋势。

（五）利用网络资源的犯罪

此类犯罪集中表现为下载网上资源进行犯罪，比较突出的是法轮功分子下载法轮功网站内容进行传播和通过互联网非法获取公民个人信息的行为。近十年本院共审结此类案件53件。

与2006年之前审结的此类案件相对比，有如下特点：

1.邪教类犯罪减少、非法获取公民信息犯罪增多。1998年到2006年利邪教破坏法律实施的共计25件，而近十年仅有15件，然而非法获取公民个人信息案件高达33件，成为网络犯罪中最常见的犯罪之一，增长势头迅猛；

2.邪教犯罪多中老年女性，非法获取公民信息多青壮年男性。利用邪教组织破坏法律实施罪的主体为中老年，女性占20%，平均年龄43岁，而在2006年之前这类犯罪人平均年龄仅有35.3岁，说明中老年人更容易被邪教蛊惑， 60%犯罪人为退休或者在职人员。非法获取公民个人信息罪的案件中犯罪者女性较少，平均年龄28岁，以无业人员为主，大专以上学历占54%，趋向高学历犯罪；

3.两类犯罪的行为方式差别大。利用邪教组织破坏法律实施罪中，行为人多是通过境外网站获取邪教宣传片，下载制作光盘、宣传册等，而非法获取公民个人信息罪的犯罪人包括出卖信息者和购买信息者，出卖者多从事招聘、中介等职业，利用工作便利将客户信息私自贩卖，购买者则多是通过网络直接找到卖家，收购个人信息用于商业目的或者诈骗，这类行为也助长电信诈骗；

4. 这类行为与利用网络作为犯罪场所的犯罪以及利用网络作为犯罪中介有竞合，部分犯罪人从网络上将资源复制后，通过网络继续散播或出售。

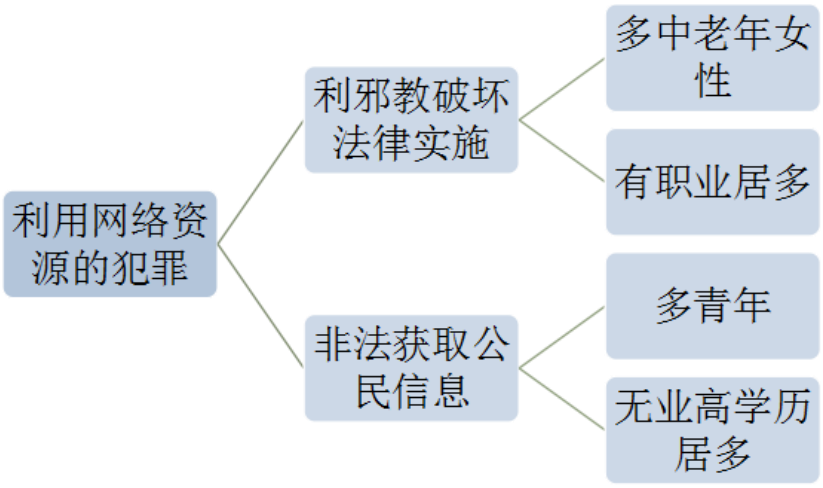

图 16 利用网络资源的犯罪分类及特点

四、 网络犯罪案件审理难点分析

1998 年至 2006 年本院调查[6]中发现，网络犯罪出现的原因主要包括三个[7]:社会成因、成本成因和技术成因。2007 至今的近十年，这三个因素依旧是网络犯罪的主要成因，此外，近十年网络犯罪增长不可忽视的成因是司法实践中的立案难、取证难、定罪难等法律成因。

[6] 详见石金平、游涛：《对海淀区人民法院审结的网络犯罪案件的情况分析》。

[7] 该调查报告中指出: 在网络空间里漫游的人们，可以毫无身份可言，有的可能只是一个虚假的身份，这个时候人们的思维或言语行为，完全脱离了家庭、熟人、所在社会组织的监控，比处于一个完全陌生的现实社会环境中的人还要自由。网络漫游者固有的社会规范、社会舆论、社会道德意识，必然会变得混乱或者被削弱，从而对个人行为模式的规范作用急剧下降或者暂时消失，网络虚拟环境为个人言行的私密性和随意性创造了发挥的空间，网络设计者会大量地设置一些低级趣味的信息或空间，以满足这些人的需求，从而更加刺激了这些人的欲求，更深刻地摧毁了人们在现实社会中存有的社会伦理道德、价值观。那些利用“黑客”程序进行犯罪的人，承认自己在成功获取了有价值信息后有了自以为聪明的快感。由于网络犯罪隐蔽性极强，法律规范不全，证据的收集和判断困难，使他们极易逃避司法追究。这使得它的风险是非常小的。同时，不管是达到目的的成功感还是巨额的财富，网络犯罪的利润都是极高的。此外网络的脆弱性表现在：（1）计算机软件系统具有开放性，攻击者可以很容易地把体现自己意志的攻击程序置入系统软件或应用软件中，从而达到攻击目的。（2）计算机中处理的数据都是由输入设备输入系统的，数据易被篡改或输入虚假数据。（3）存储在计算机系统中的数据极易被修改和破坏。（4）经处理后的数据可通过各种输出设备输出，信息可能被泄漏或被截取。（5）在计算机网络系统中是通过通信线路传送数据，实现资源共享的，在通信线路上信息易被截取。（6）计算机设备可以向外辐射电磁波，其辐射的电磁波中带有信息，容易被人接收，造成信息泄漏。

互联网的飞速发展给传统法制体系带来非常多的挑战。立法、司法的滞后性和也给网络犯罪提供了蔓延的机遇。

结合本院的调研，可以看出网络犯罪从把网络作为犯罪对象，到一步步和传统犯罪融合，使网络成为传统犯罪的工具、场所和手段，甚至成为犯罪场所，这也使得认定网络犯罪存在很多难点。

（一） 主观构成要件认定上的难题

网络犯罪中主观构成要件认定存在被告人违法性认识不足，间接故意认定难的新问题，这是新型犯罪对传统理论的挑战。

1. 被告人违法性认识不足能否阻却定罪。网络犯罪中破坏计算机信息系统数据罪、非法获取计算机信息系统数据罪、非法控制计算机信息系统数据罪、扰乱无线电通讯管理秩序罪等新型网络犯罪，完全不同于传统犯罪，虽然刑法对此有修正案进行补充规定，但在互联网虚拟空间里，人们固有的社会规范、伦理道德、价值观很容易被削弱，对某些网络犯罪行为的犯罪感虚无化。而且在互联网兴起之后，相关法律的模糊或者滞后导致行为人并未将自己的违法犯罪行为视为违法。

以本院近期审结的一起非法获取计算机信息系统数据案件[8]为例，被告人何某毕业于知名大学，通过侵入某公司后台获取数据资源，并把获取的系统漏洞情况写入自己的研究文章，发表在乌云网，被告人辩称自己仅仅是为了测试系统漏洞，这是为了网络安全的需要是

[8] 参见（2016）京 0108 刑初 607 号刑事判决书。

“白帽子”[9]而非盗取信息数据。这种心理普遍存在于“黑客”群体中，也能引得部分网民的共鸣。

此外，利用“伪基站”发送广告短信和诈骗短信的案件中，参与发送者多是一些小公司的员工，这些员工往往辩称自己仅仅是履行职务行为，并不知道自己参与了犯罪。这些违法性认识的不足为认定犯罪人是否具有犯罪主观构成要件提出了挑战。

2.间接故意与技术中立如何区分。间接故意主要存在于网络服务提供者的实施的犯罪上，部分互联网企业为了迎合用户的趣味以实现盈利，突破传统的法律规则和公序良俗的道德伦理，对自己应该履行的管理、监管义务放任不管，以技术中立为自己开脱责任。例如快播公司传播淫秽物品牟利一案中，高管均以自己没有明知服务器存储淫秽视频资料和没有放任为自己辩解，但这这样确实给审判者认定嫌疑人是否具有主观构成要件提出难题。

（二）危害结果的确定的难题

网络犯罪中存在危害后果确定困难的问题，主要是虚拟财物如何认定数额和危害后果取证难。

1.虚拟财物认定的困难。非法获取的虚拟财物如何认定犯罪数额，直接关系到量刑档次，这也成为控辩双方的争议点之一，这在盗取游戏币的犯罪中极为常见。因为虚拟财产的价值确定有相当的难度，虚拟与现实财产之间的联系是存在变化因素的，比方游戏币这种

[9]白帽子是指正面的黑客，可以识别计算机系统或网络系统中的安全漏洞，但并不会恶意去利用，而是公布其漏洞。

虚拟财产，其与游戏的性质、运营状况、运营成本密切相关，所以在具体案件中如何认定虚拟财产实际价值十分困难。例如本院审结的吴某非法获取计算机信息系统数据罪一案[10]中，吴某利用游戏网站充值漏洞以远低于游戏定价的金额充值获取大量游戏币，并将游戏币以略低于游戏定价的价格在淘宝变卖，这一案件中被害游戏公司要求按照被告人获取游戏币的数量和公司定价认定损失，而检察官将被告人实际获利作为定罪金额。这也成为审理的难点之一

2. 造成损失无法确定。犯罪危害后果，除了现实的损失，后续的危害也是不可估量。传统犯罪囿于空间和有限资源，对犯罪客观上存在有形或者无形的各种约束，而网络资源的和空间的无限性，使得犯罪行为能无限复制，比如计算机病毒被编写后，虽然犯罪人被控制，但是感染病毒的计算机的数量和后续被侵害的计算机无法估量。此外，在电信诈骗中，现实社会的实施诈骗的自然人或者单位变成了虚拟的 IP 地址和域名，侦查中人机对应的同一性认定存在困难，加上受害者往往遍布各地，单个案件往往无法达到立案标准。而并案则对现有侦查取证提出更高要求，如果存在服务器设在境外的情形更增加侦查工作量和取证难度。跨地域立案与并案也存在客观难度，使得犯罪所得数额难以确定。最后定案数额往往比实际非法获利相差甚多，而重罪轻判会给其他犯罪分子铤而走险的心理激励。再者，电子证据的存储和调取都存在现实的约束和技术的瓶颈，如出租僵尸网络非法

[10] 参见（2015）海刑初字第 1931 号刑事判决书。

控制他人计算机实施 DDOS 攻击时，往往由于机器不存在日志记录，而且抓取的僵尸机处于动态变化中，给认定实际控制计算机和损失数额带来困难。

（三）行为定性的难题

新型网络犯罪行为定性上往往存在争议，包括利用网络漏洞盗取游戏币或者虚假充值等行为，在审判中和学术上都存在是定性为盗窃罪、诈骗罪、非法获取计算机信息数据罪的争议。

此外，帮助行为能否正犯化也是一个争议点。传统刑法理论认为共同犯罪需要具备共同犯罪故意和共同犯罪行为。但在网络犯罪中，行为人之间意思联络形式多样化、联络主体虚拟化、共同行为模糊化，很难套用传统刑法对共同犯罪构成要件的要求。而大量存在的帮助行为，例如恶意链接帮助了淫秽诈骗等违法信息的传播与扩散，使得分散的违法信息聚集，其帮助行为的危害程度已经出现社会危害性聚拢、集聚、强化的作用。此类帮助行为由于社会危害性的升高，是否给予正犯化处理，急需解释。

五、审判中的应对之策

针对调研中发现的审理中的难题，结合我院审判实践，可以从以下几点做出应对：

（一）违法性认识不足不妨碍主观构成要件认定

刑法理论中将违法性认识作为认识错误的一种，但是在网络犯罪中行为人能熟练运用计算机，往往具有高学历，并且可以通过网络获

取信息，并不能以此作为抗辩的理由。所以，对于辩称自己主观动机仅仅是发现漏洞的黑客，只要实施了刑法所禁止的其他犯罪行为，依然按照客观行为和主观故意定罪。至于没有造成严重社会危害则是在量刑中酌情考量的情节。

（二）技术中立不能是间接故意的挡箭牌

网络企业、服务提供者等运营、维护主体都具有自我监管的义务，虽然在互联网领域，存在“技术中立原则”，就是技术提供者只要不知道也没有合理的理由应当知道技术被用于侵权，就可以免于承担连带处罚。但是如果技术被用于侵权，而服务提供者显然知晓却惰于监管，放任危害结果，以致触及刑法底线，毫无意外是间接故意。以“快播”案为典型，这证明王欣对快播网络传播淫秽视频的事实不但明知，而且还着手采取规避检查的技术措施，消极对待监管责任，放任大量淫秽视频经由其网络系统、缓存服务器大量传播。”审判长表示，快播公司及被告人的行为构成了主观故意中的“间接故意”

（三）犯罪危害后果的认定

网络犯罪危害结果的取证难时现阶段客观存在的问题，破解它需要侦查机关投入大量人力、物力，无法在短期内能取得巨大的提升，所以依据现有侦查条件，在审理中认定虚拟财物价值时，需要由价格鉴定机构进行专业认定，不能仅依据被害人提供价格标准或者被告人的实际获利认定犯罪数额，这样才能客观。此外，犯罪的直接损失往往有形，比如认定破坏计算机信息系统罪的案件中，被害公司为修复

遭到破坏的漏洞所支付的维护费用就是显而易见的直接损失。但是间接损失则往往无法量化，需要审判者酌情考虑。

（四）案件定性的解决

案件的定性需要结合典型案例，比方如何区分盗窃和非法获取计算机信息系统数据罪，我院的审结案例中将盗窃实际财物的网络侵入行为定为盗窃，而将虚拟财物视为信息数据，将此类行为定罪为非法获取计算机信息系统数据罪。

涉及共犯问题，如果是计算机仅仅是行为人的犯罪工具，行为人在符合相应的犯罪构成的情况下，要按照对应的罪名进行定罪处罚，如果行为人提供“中性业务行为”如单纯的互联网接入、服务器托管、网络存储、通讯技术、广告推广、支付结算等互联网基础服务，没有产生诈骗、盗窃之类的共同犯罪意思，则适用《刑修九》刚刚修正的“帮助信息网络犯罪活动罪”。