**最高人民检察院第十八批指导性案例**

**张凯闵等52人电信网络诈骗案**

**（检例第67号）**

**【关键词】**

跨境电信网络诈骗 境外证据审查 电子数据 引导取证

**【要旨】**

跨境电信网络诈骗犯罪往往涉及大量的境外证据和庞杂的电子数据。对境外获取的证据应着重审查合法性，对电子数据应着重审查客观性。主要成员固定，其他人员有一定流动性的电信网络诈骗犯罪组织，可认定为犯罪集团。

**【基本案情】**

被告人张凯闵，男，1981年11月21日出生，中国台湾地区居民，无业。

林金德等其他被告人、被不起诉人基本情况略。

2015年6月至2016年4月间，被告人张凯闵等52人先后在印度尼西亚共和国和肯尼亚共和国参加对中国大陆居民进行电信网络诈骗的犯罪集团。在实施电信网络诈骗过程中，各被告人分工合作，其中部分被告人负责利用电信网络技术手段对大陆居民的手机和座机电话进行语音群呼，群呼的主要内容为“有快递未签收，经查询还有护照签证即将过期，将被限制出境管制，身份信息可能遭泄露”等。当被害人按照语音内容操作后，电话会自动接通冒充快递公司客服人员的一线话务员。一线话务员以帮助被害人报案为由，在被害人不挂断电话时，将电话转接至冒充公安局办案人员的二线话务员。二线话务员向被害人谎称“因泄露的个人信息被用于犯罪活动，需对被害人资金流向进行调查”，欺骗被害人转账、汇款至指定账户。如果被害人对二线话务员的说法仍有怀疑，二线话务员会将电话转给冒充检察官的三线话务员继续实施诈骗。

至案发，张凯闵等被告人通过上述诈骗手段骗取75名被害人钱款共计人民币2300余万元。

**【指控与证明犯罪】**

（一）介入侦查引导取证

由于本案被害人均是中国大陆居民，根据属地管辖优先原则，2016年4月，肯尼亚将76名电信网络诈骗犯罪嫌疑人（其中大陆居民32人，台湾地区居民44人）遣返中国大陆。经初步审查，张凯闵等41人与其他被遣返的人分属互不关联的诈骗团伙，公安机关依法分案处理。2016年5月，北京市人民检察院第二分院经指定管辖本案，并应公安机关邀请，介入侦查引导取证。

鉴于肯尼亚在遣返犯罪嫌疑人前已将起获的涉案笔记本电脑、语音网关（指能将语音通信集成到数据网络中实现通信功能的设备）、手机等物证移交我国公安机关，为确保证据的客观性、关联性和合法性，检察机关就案件证据需要达到的证明标准以及涉外电子数据的提取等问题与公安机关沟通，提出提取、恢复涉案的Skype聊天记录、Excel和Word文档、网络电话拨打记录清单等电子数据，并对电子数据进行无污损鉴定的意见。在审查电子数据的过程中，检察人员与侦查人员在恢复的Excel文档中找到多份“返乡订票记录单”以及早期大量的Skype聊天记录。依据此线索，查实部分犯罪嫌疑人在去肯尼亚之前曾在印度尼西亚两度针对中国大陆居民进行诈骗，诈骗数额累计达2000余万元人民币。随后，11名曾在印度尼西亚参与张凯闵团伙实施电信诈骗，未赴肯尼亚继续诈骗的犯罪嫌疑人陆续被缉捕到案。至此，张凯闵案52名犯罪嫌疑人全部到案。

（二）审查起诉

审查起诉期间，在案犯罪嫌疑人均表示认罪，但对其在犯罪集团中的作用和参与犯罪数额各自作出辩解。

经审查，北京市人民检察院第二分院认为现有证据足以证实张凯闵等人利用电信网络实施诈骗，但案件证据还存在以下问题：一是电子数据无污损鉴定意见的鉴定起始基准时间晚于犯罪嫌疑人归案的时间近11个小时，不能确定在此期间电子数据是否被增加、删除、修改。二是被害人与诈骗犯罪组织间的关联性证据调取不完整，无法证实部分被害人系本案犯罪组织所骗。三是台湾地区警方提供的台湾地区犯罪嫌疑人出入境记录不完整，北京市公安局出入境管理总队出具的出入境记录与犯罪嫌疑人的供述等其他证据不尽一致，现有证据不能证实各犯罪嫌疑人参加诈骗犯罪组织的具体时间。

针对上述问题，北京市人民检察院第二分院于2016年12月17日、2017年3月7日两次将案件退回公安机关补充侦查，并提出以下补充侦查意见：一是通过中国驻肯尼亚大使馆确认抓获犯罪嫌疑人和外方起获物证的具体时间，将此时间作为电子数据无污损鉴定的起始基准时间，对电子数据重新进行无污损鉴定，以确保电子数据的客观性。二是补充调取犯罪嫌疑人使用网络电话与被害人通话的记录、被害人向犯罪嫌疑人指定银行账户转账汇款的记录、犯罪嫌疑人的收款账户交易明细等证据，以准确认定本案被害人。三是调取各犯罪嫌疑人护照，由北京市公安局出入境管理总队结合护照，出具完整的出入境记录，补充讯问负责管理护照的犯罪嫌疑人，核实部分犯罪嫌疑人是否中途离开过诈骗窝点，以准确认定各犯罪嫌疑人参加犯罪组织的具体时间。补充侦查期间，检察机关就补侦事项及时与公安机关加强当面沟通，落实补证要求。与此同时，检察人员会同侦查人员共赴国家信息中心电子数据司法鉴定中心，就电子数据提取和无污损鉴定等问题向行业专家咨询，解决了无污损鉴定的具体要求以及提取、固定电子数据的范围、程序等问题。检察机关还对公安机关以《司法鉴定书》记录电子数据勘验过程的做法提出意见，要求将《司法鉴定书》转化为勘验笔录。通过上述工作，全案证据得到进一步完善，最终形成补充侦查卷21册，为案件的审查和提起公诉奠定了坚实基础。

检察机关经审查认为，根据肯尼亚警方出具的《调查报告》、我国驻肯尼亚大使馆出具的《情况说明》以及公安机关出具的扣押决定书、扣押清单等，能够确定境外获取的证据来源合法，移交过程真实、连贯、合法。国家信息中心电子数据司法鉴定中心重新作出的无污损鉴定，鉴定的起始基准时间与肯尼亚警方抓获犯罪嫌疑人并起获涉案设备的时间一致，能够证实电子数据的真实性。涉案笔记本电脑和手机中提取的Skype账户登录信息等电子数据与犯罪嫌疑人的供述相互印证，能够确定犯罪嫌疑人的网络身份和现实身份具有一致性。75名被害人与诈骗犯罪组织间的关联性证据已补充到位，具体表现为：网络电话、Skype聊天记录等与被害人陈述的诈骗电话号码、银行账号等证据相互印证；电子数据中的聊天时间、通话时间与银行交易记录中的转账时间相互印证；被害人陈述的被骗经过与被告人供述的诈骗方式相互印证。本案的75名被害人被骗的证据均满足上述印证关系。

（三）出庭指控犯罪

2017年4月1日，北京市人民检察院第二分院根据犯罪情节，对该诈骗犯罪集团中的52名犯罪嫌疑人作出不同处理决定。对张凯闵等50人以诈骗罪分两案向北京市第二中级人民法院提起公诉，对另2名情节较轻的犯罪嫌疑人作出不起诉决定。7月18日、7月19日，北京市第二中级人民法院公开开庭审理了本案。

庭审中，50名被告人对指控的罪名均未提出异议，部分被告人及其辩护人主要提出以下辩解及辩护意见：一是认定犯罪集团缺乏法律依据，应以被告人实际参与诈骗成功的数额认定其犯罪数额。二是被告人系犯罪组织雇佣的话务员，在本案中起次要和辅助作用，应认定为从犯。三是检察机关指控的犯罪金额证据不足，没有形成完整的证据链条，不能证明被害人是被告人所骗。

针对上述辩护意见，公诉人答辩如下：

一是该犯罪组织以共同实施电信网络诈骗犯罪为目的而组建，首要分子虽然没有到案，但在案证据充分证明该犯罪组织在首要分子的领导指挥下，有固定人员负责窝点的组建管理、人员的召集培训，分工担任一线、二线、三线话务员，该诈骗犯罪组织符合刑法关于犯罪集团的规定，应当认定为犯罪集团。

二是在案证据能够证实二线、三线话务员不仅实施了冒充警察、检察官接听拨打电话的行为，还在犯罪集团中承担了组织管理工作，在共同犯罪中起主要作用，应认定为主犯。对从事一线接听拨打诈骗电话的被告人，已作区别对待。该犯罪集团在印度尼西亚和肯尼亚先后设立3个窝点，参加过2个以上窝点犯罪的一线人员属于积极参加犯罪，在犯罪中起主要作用，应认定为主犯；仅参加其中一个窝点犯罪的一线人员，参与时间相对较短，实际获利较少，可认定为从犯。

三是本案认定诈骗犯罪集团与被害人之间关联性的证据主要有：犯罪集团使用网络电话与被害人电话联系的通话记录；犯罪集团的Skype聊天记录中提到了被害人姓名、公民身份号码等个人信息；被害人向被告人指定银行账户转账汇款的记录。起诉书认定的75名被害人至少包含上述一种关联方式，实施诈骗与被骗的证据能够形成印证关系，足以认定75名被害人被本案诈骗犯罪组织所骗。

（四）处理结果

2017年12月21日，北京市第二中级人民法院作出一审判决，认定被告人张凯闵等50人以非法占有为目的，参加诈骗犯罪集团，利用电信网络技术手段，分工合作，冒充国家机关工作人员或其他单位工作人员，诈骗被害人钱财，各被告人的行为均已构成诈骗罪，其中28人系主犯，22人系从犯。法院根据犯罪事实、情节并结合各被告人的认罪态度、悔罪表现，对张凯闵等50人判处十五年至一年九个月不等有期徒刑，并处剥夺政治权利及罚金。张凯闵等部分被告人以量刑过重为由提出上诉。2018年3月，北京市高级人民法院二审裁定驳回上诉，维持原判。

**【指导意义】**

（一）对境外实施犯罪的证据应着重审查合法性

对在境外获取的实施犯罪的证据，一是要审查是否符合我国刑事诉讼法的相关规定，对能够证明案件事实且符合刑事诉讼法规定的，可以作为证据使用。二是对基于有关条约、司法互助协定、两岸司法互助协议或通过国际组织委托调取的证据，应注意审查相关办理程序、手续是否完备，取证程序和条件是否符合有关法律文件的规定。对不具有规定规范的，一般应当要求提供所在国公证机关证明，由所在国中央外交主管机关或其授权机关认证，并经我国驻该国使、领馆认证。三是对委托取得的境外证据，移交过程中应注意审查过程是否连续、手续是否齐全、交接物品是否完整、双方的交接清单记载的物品信息是否一致、交接清单与交接物品是否一一对应。四是对当事人及其辩护人、诉讼代理人提供的来自境外的证据材料，要审查其是否按照条约等相关规定办理了公证和认证，并经我国驻该国使、领馆认证。

（二）对电子数据应重点审查客观性

一要审查电子数据存储介质的真实性。通过审查存储介质的扣押、移交等法律手续及清单，核实电子数据存储介质在收集、保管、鉴定、检查等环节中是否保持原始性和同一性。二要审查电子数据本身是否客观、真实、完整。通过审查电子数据的来源和收集过程，核实电子数据是否从原始存储介质中提取，收集的程序和方法是否符合法律和相关技术规范。对从境外起获的存储介质中提取、恢复的电子数据应当进行无污损鉴定，将起获设备的时间作为鉴定的起始基准时间，以保证电子数据的客观、真实、完整。三要审查电子数据内容的真实性。通过审查在案言词证据能否与电子数据相互印证，不同的电子数据间能否相互印证等，核实电子数据包含的案件信息能否与在案的其他证据相互印证。

（三）紧紧围绕电话卡和银行卡审查认定案件事实

办理电信网络诈骗犯罪案件，认定被害人数量及诈骗资金数额的相关证据，应当紧紧围绕电话卡和银行卡等证据的关联性来认定犯罪事实。一是通过电话卡建立被害人与诈骗犯罪组织间的关联。通过审查诈骗犯罪组织使用的网络电话拨打记录清单、被害人接到诈骗电话号码的陈述以及被害人提供的通话记录详单等通讯类证据，认定被害人与诈骗犯罪组织间的关联性。二是通过银行卡建立被害人与诈骗犯罪组织间的关联。通过审查被害人提供的银行账户交易明细、银行客户通知书、诈骗犯罪集团指定银行账户信息等书证以及诈骗犯罪组织使用的互联网软件聊天记录，核实聊天记录中是否出现被害人的转账账户，以确定被害人与诈骗犯罪组织间的关联性。三是将电话卡和银行卡结合起来认定被害人及诈骗数额。审查被害人接到诈骗电话的时间、向诈骗犯罪组织指定账户转款的时间，诈骗犯罪组织手机或电脑中储存的聊天记录中出现的被害人的账户信息和转账时间是否印证。相互关联印证的，可以认定为案件被害人，被害人实际转账的金额可以认定为诈骗数额。

（四）有明显首要分子，主要成员固定，其他人员有一定流动性的电信网络诈骗犯罪组织，可以认定为诈骗犯罪集团

实施电信网络诈骗犯罪，大都涉案人员众多、组织严密、层级分明、各环节分工明确。对符合刑法关于犯罪集团规定，有明确首要分子，主要成员固定，其他人员虽有一定流动性的电信网络诈骗犯罪组织，依法可以认定为诈骗犯罪集团。对出资筹建诈骗窝点、掌控诈骗所得资金、制定犯罪计划等起组织、指挥管理作用的，依法可以认定为诈骗犯罪集团首要分子，按照集团所犯的全部罪行处罚。对负责协助首要分子组建窝点、招募培训人员等起积极作用的，或加入时间较长，通过接听拨打电话对受害人进行诱骗，次数较多、诈骗金额较大的，依法可以认定为主犯，按照其参与或组织、指挥的全部犯罪处罚。对诈骗次数较少、诈骗金额较小，在共同犯罪中起次要或者辅助作用的，依法可以认定为从犯，依法从轻、减轻或免除处罚。

**【相关规定】**

《中华人民共和国刑法》第六条、第二十六条、第二百六十六条

《中华人民共和国刑事诉讼法》第十八条、第二十五条

《中华人民共和国国际刑事司法协助法》第九条、第十条、第二十五条、第二十六条、第三十九条、第四十条、第四十一条、第六十八条

《最高人民法院、最高人民检察院、公安部关于办理诈骗刑事案件具体应用法律若干问题的解释》第一条、第二条

《最高人民法院、最高人民检察院、公安部关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》

《最高人民法院、最高人民检察院、公安部关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》

《检察机关办理电信网络诈骗案件指引》

《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》第四百零五条

**叶源星、张剑秋提供侵入计算机信息系统程序、谭房妹非法获取计算机信息系统数据案**

**（检例第68号）**

**【关键词】**

专门用于侵入计算机信息系统的程序 非法获取计算机信息系统数据 撞库 打码

**【要旨】**

对有证据证明用途单一，只能用于侵入计算机信息系统的程序，司法机关可依法认定为“专门用于侵入计算机信息系统的程序”；难以确定的，应当委托专门部门或司法鉴定机构作出检验或鉴定。

**【基本案情】**

叶源星，男，1977年3月10日出生，超市网络维护员。

张剑秋，男，1972年8月14日出生，小学教师。

谭房妹，男，1993年4月5日出生，农民。

2015年1月，被告人叶源星编写了用于批量登录某电商平台账户的“小黄伞”撞库软件（“撞库”是指黑客通过收集已泄露的用户信息，利用账户使用者相同的注册习惯，如相同的用户名和密码，尝试批量登陆其他网站，从而非法获取可登录用户信息的行为）供他人免费使用。“小黄伞”撞库软件运行时，配合使用叶源星编写的打码软件（“打码”是指利用人工大量输入验证码的行为）可以完成撞库过程中对大量验证码的识别。叶源星通过网络向他人有偿提供打码软件的验证码识别服务，同时将其中的人工输入验证码任务交由被告人张剑秋完成，并向其支付费用。

2015年1月至9月，被告人谭房妹通过下载使用“小黄伞”撞库软件，向叶源星购买打码服务，获取到某电商平台用户信息2.2万余组。

被告人叶源星、张剑秋通过实施上述行为，从被告人谭房妹处获取违法所得共计人民币4万余元。谭房妹通过向他人出售电商平台用户信息，获取违法所得共计人民币25万余元。法院审理期间，叶源星、张剑秋、谭房妹退缴了全部违法所得。

**【指控与证明犯罪】**

（一）审查起诉

2016年10月10日，浙江省杭州市公安局余杭区分局以犯罪嫌疑人叶源星、张剑秋、谭房妹涉嫌非法获取计算机信息系统数据罪移送杭州市余杭区人民检察院审查起诉。期间，叶源星、张剑秋的辩护人向检察机关提出二名犯罪嫌疑人无罪的意见。叶源星的辩护人认为，叶源星利用“小黄伞”软件批量验证已泄露信息的行为，不构成非法获取计算机信息系统数据罪。张剑秋的辩护人认为，张剑秋不清楚组织打码是为了非法获取某电商平台的用户信息。张剑秋与叶源星没有共同犯罪故意，不构成非法获取计算机信息系统数据罪。

杭州市余杭区人民检察院经审查认为，犯罪嫌疑人叶源星编制“小黄伞”撞库软件供他人使用，犯罪嫌疑人张剑秋组织码工打码，犯罪嫌疑人谭房妹非法获取网络用户信息并出售牟利的基本事实清楚，但需要进一步补强证据。2016年11月25日、2017年2月7日，检察机关二次将案件退回公安机关补充侦查，明确提出需要补查的内容、目的和要求。一是完善“小黄伞”软件的编制过程、运作原理、功能等方面的证据，以便明确“小黄伞”软件是否具有避开或突破某电商平台服务器的安全保护措施，非法获取计算机信息系统数据的功能。二是对扣押的张剑秋电脑进行补充勘验，以便确定张剑秋主观上是否明知其组织打码行为是为他人非法获取某电商平台用户信息提供帮助；调取张剑秋与叶源星的QQ聊天记录，以便查明二人是否有犯意联络。三是提取叶源星被扣押电脑的MAC地址（又叫网卡地址，由12个16进制数组成，是上网设备在网络中的唯一标识），分析“小黄伞”软件源代码中是否含有叶源星电脑的MAC地址，以便查明某电商平台被非法登陆过的账号与叶源星编制的“小黄伞”撞库软件之间是否存在关联性。四是对被扣押的谭房妹电脑和U盘进行补充勘验，调取其中含有账号、密码的文件，查明文件的生成时间和特征，以便确定被查获的存储介质中的某电商平台用户信息是否系谭房妹使用“小黄伞”软件获取。

公安机关按照检察机关的要求，对证据作了进一步补充完善。同时，检察机关就“小黄伞”软件的运行原理等问题，听取了技术专家意见。结合公安机关两次退查后补充的证据，案件证据中存在的问题已经得到解决：

一是明确了 “小黄伞”软件具有以下功能特征：（1）“小黄伞”软件用途单一，仅针对某电商平台账号进行撞库和接入打码平台，这种非法侵入计算机信息系统获取用户数据的程序没有合法用途。（2）“小黄伞”软件具有避开或突破计算机信息系统安全保护措施的功能。在实施撞库过程中，一个IP地址需要多次登录大量账号，为防止被某电商平台识别为非法登陆，导致IP地址被封锁，“小黄伞”软件被编入自动拨号功能，在批量登陆几组账号后，会自动切换新的IP地址，从而达到避开该电商平台安全防护的目的。（3）“小黄伞”软件具有绕过验证码识别防护措施的功能。在他人利用非法获取的该电商平台账号登录时，需要输入验证码。“小黄伞”软件会自动抓取验证码图片发送到打码平台，由张剑秋组织的码工对验证码进行识别。（4）“小黄伞”软件具有非法获取计算机信息系统数据的功能。“小黄伞”软件对登陆成功的某电商平台账号，在未经授权的情况下，会自动抓取账号对应的昵称、注册时间、账号等级等信息数据。根据以上特征，可以认定“小黄伞”软件属于刑法规定的“专门用于侵入计算机信息系统的程序”。

二是从张剑秋和叶源星电脑中补充勘查到的QQ聊天记录等电子数据证实，叶源星与张剑秋聊天过程中曾提及“扫平台”、“改一下平台程序”、“那些人都是出码的”；通过补充讯问张剑秋和叶源星，明确了张剑秋明知其帮叶源星打验证码可能被用于非法目的，仍然帮叶源星做打码代理。上述证据证实张剑秋与叶源星之间已经形成犯意联络，具有共同犯罪故意。

三是通过进一步补充证据，证实了使用撞库软件的终端设备的MAC地址与叶源星电脑的MAC地址、小黄伞软件的源代码里包含的MAC地址一致。上述证据证实叶源星就是“小黄伞”软件的编制者。

四是通过对谭房妹所有包含某电商平台用户账号和密码的文件进行比对，查明了谭房妹利用“小黄伞”撞库软件非法获取的某电商平台用户信息文件不仅包含账号、密码，还包含了注册时间、账号等级、是否验证等信息，而谭房妹从其他渠道非法获取的账号信息文件并不包含这些信息。通过对谭房妹电脑的进一步勘查和对谭房妹的进一步讯问，确定了谭房妹利用“小黄伞”软件登陆某电商平台用户账号的过程和具体时间，该登录时间与部分账号信息文件的生成时间均能一一对应。根据上述证据，最终确定谭房妹利用“小黄伞”撞库所得的网络用户信息为2.2万余组。

综上，检察机关认为案件事实已查清，但公安机关对犯罪嫌疑人叶源星、张剑秋移送起诉适用的罪名不准确。叶源星、张剑秋共同为他人提供专门用于侵入计算机信息系统的程序，均已涉嫌提供侵入计算机信息系统程序罪；犯罪嫌疑人谭房妹的行为已涉嫌非法获取计算机信息系统数据罪。

（二）出庭指控犯罪

2017年6月20日，杭州市余杭区人民检察院以被告人叶源星、张剑秋构成提供侵入计算机信息系统程序罪，被告人谭房妹构成非法获取计算机信息系统数据罪，向杭州市余杭区人民法院提起公诉。11月17日，法院公开开庭审理了本案。

庭审中，3名被告人对检察机关的指控均无异议。谭房妹的辩护人提出，谭房妹系初犯，归案后能如实供述罪行，自愿认罪，请求法庭从轻处罚。叶源星和张剑秋的辩护人提出以下辩护意见：一是检察机关未提供省级以上有资质机构的检验结论，现有证据不足以认定“小黄伞”软件是“专门用于侵入计算机信息系统的程序”。二是张剑秋与叶源星间没有共同犯罪的主观故意。三是叶源星和张剑秋的违法所得金额应扣除支付给码工的钱款。

针对上述辩护意见，公诉人答辩如下：一是在案电子数据、勘验笔录、技术人员的证言、被告人供述等证据相互印证，足以证实“小黄伞”软件具有避开和突破计算机信息系统安全保护措施，未经授权获取计算机信息系统数据的功能，属于法律规定的“专门用于侵入计算机信息系统的程序”。二是被告人叶源星与张剑秋具有共同犯罪的故意。QQ聊天记录反映两人曾提及非法获取某电商平台用户信息的内容，能证实张剑秋主观明知其组织他人打码系用于批量登录该电商平台账号。张剑秋组织他人帮助打码的行为和叶源星提供撞库软件的行为相互配合，相互补充，系共同犯罪。三是被告人叶源星、张剑秋的违法所得应以其出售验证码服务的金额认定，给码工等相关支出均属于犯罪成本，不应扣除。二人系共同犯罪，应当对全部犯罪数额承担责任。四是3名被告人在庭审中认罪态度较好且上交了全部违法所得，建议从轻处罚。

（三）处理结果

浙江省杭州市余杭区人民法院采纳了检察机关的指控意见，判决认定被告人叶源星、张剑秋的行为已构成提供侵入计算机信息系统程序罪，且系共同犯罪；被告人谭房妹的行为已构成非法获取计算机信息系统数据罪。鉴于3名被告人均自愿认罪，并退出违法所得，对3名被告人判处三年有期徒刑，适用缓刑，并处罚金。宣判后，3名被告人均未提出上诉，判决已生效。

**【指导意义】**

审查认定“专门用于侵入计算机信息系统的程序”，一般应要求公安机关提供以下证据：一是从被扣押、封存的涉案电脑、U盘等原始存储介质中收集、提取相关的电子数据。二是对涉案程序、被侵入的计算机信息系统及电子数据进行勘验、检查后制作的笔录。三是能够证实涉案程序的技术原理、制作目的、功能用途和运行效果的书证材料。四是涉案程序的制作人、提供人、使用人对该程序的技术原理、制作目的、功能用途和运行效果进行阐述的言词证据，或能够展示涉案程序功能的视听资料。五是能够证实被侵入计算机信息系统安全保护措施的技术原理、功能以及被侵入后果的专业人员的证言等证据。六是对有运行条件的，应要求公安机关进行侦查实验。对有充分证据证明涉案程序是专门设计用于侵入计算机信息系统、非法获取计算机信息系统数据的，可直接认定为“专门用于侵入计算机信息系统的程序”。

证据审查中，可从以下方面对涉案程序是否属于“专门用于侵入计算机信息系统的程序”进行判断：一是结合被侵入的计算机信息系统的安全保护措施，分析涉案程序是否具有侵入的目的，是否具有避开或者突破计算机信息系统安全保护措施的功能。二是结合计算机信息系统被侵入的具体情形，查明涉案程序是否在未经授权或超越授权的情况下，获取计算机信息系统数据。三是分析涉案程序是否属于“专门”用于侵入计算机信息系统的程序。

根据《最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》第十条和《最高人民法院、最高人民检察院、公安部关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》第十七条的规定，对是否属于“专门用于侵入计算机信息系统的程序”难以确定的，一般应当委托省级以上负责计算机信息系统安全保护管理工作的部门检验，也可由司法鉴定机构出具鉴定意见，或者由公安部指定的机构出具报告。实践中，应重点审查检验报告、鉴定意见对程序运行过程和运行结果的判断，结合案件具体情况，认定涉案程序是否具有突破或避开计算机信息系统安全保护措施，未经授权或超越授权获取计算机信息系统数据的功能。

**【相关规定】**

《中华人民共和国刑法》第二百八十五条、第二十五条

《最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》第一条、第二条、第三条、第十条、第十一条

《最高人民法院、最高人民检察院、公安部关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》第十七条

**姚晓杰等11人破坏计算机信息系统案**

**（检例第69号）**

**【关键词】**

破坏计算机信息系统　网络攻击 引导取证 损失认定

**【要旨】**

为有效打击网络攻击犯罪，检察机关应加强与公安机关的配合，及时介入侦查引导取证，结合案件特点提出明确具体的补充侦查意见。对被害互联网企业提供的证据和技术支持意见，应当结合其他证据进行审查认定，客观全面准确认定破坏计算机信息系统罪的危害后果。

**【基本案情】**

被告人姚晓杰，男，1983年3月27日出生，无固定职业。

被告人丁虎子，男，1998年2月7日出生，无固定职业。

其他9名被告人基本情况略。

2017年初，被告人姚晓杰等人接受王某某（另案处理）雇佣，招募多名网络技术人员，在境外成立“暗夜小组”黑客组织。“暗夜小组”从被告人丁虎子等3人处购买大量服务器资源，再利用木马软件操控控制端服务器实施DDoS攻击（指黑客通过远程控制服务器或计算机等资源，对目标发动高频服务请求，使目标服务器因来不及处理海量请求而瘫痪）。2017年2—3月间，“暗夜小组”成员三次利用14台控制端服务器下的计算机，持续对某互联网公司云服务器上运营的三家游戏公司的客户端IP进行DDoS攻击。攻击导致三家游戏公司的IP被封堵，出现游戏无法登录、用户频繁掉线、游戏无法正常运行等问题。为恢复云服务器的正常运营，某互联网公司组织人员对服务器进行了抢修并为此支付4万余元。

**【指控与证明犯罪】**

（一）介入侦查引导取证

2017年初，某互联网公司网络安全团队在日常工作中监测到多起针对该公司云服务器的大流量高峰值DDoS攻击，攻击源IP地址来源不明，该公司随即报案。公安机关立案后，同步邀请广东省深圳市人民检察院介入侦查、引导取证。

针对案件专业性、技术性强的特点，深圳市人民检察院会同公安机关多次召开案件讨论会，就被害单位云服务器受到的DDoS攻击的特点和取证策略进行研究，建议公安机关及时将被害单位报案提供的电子数据送国家计算机网络应急技术处理协调中心广东分中心进行分析，确定主要攻击源的IP地址。

2017年6—9月间，公安机关陆续将11名犯罪嫌疑人抓获。侦查发现，“暗夜小组”成员为逃避打击，在作案后已串供并将手机、笔记本电脑等作案工具销毁或者进行了加密处理。“暗夜小组”成员到案后大多作无罪辩解。有证据证实丁虎子等人实施了远程控制大量计算机的行为，但证明其将控制权出售给“暗夜小组”用于DDoS网络攻击的证据薄弱。

鉴于此，深圳市检察机关与公安机关多次会商研究“暗夜小组”团伙内部结构、犯罪行为和技术特点等问题，建议公安机关重点做好以下三方面工作：一是查明导致云服务器不能正常运行的原因与“暗夜小组”攻击行为间的关系。具体包括：对被害单位提供的受攻击IP和近20万个攻击源IP作进一步筛查分析，找出主要攻击源的IP地址，并与丁虎子等人出售的控制端服务器IP地址进行比对；查清主要攻击源的波形特征和网络协议，并和丁虎子等人控制的攻击服务器特征进行比对，以确定主要攻击是否来自于该控制端服务器；查清攻击时间和云服务器因被攻击无法为三家游戏公司提供正常服务的时间；查清攻击的规模；调取“暗夜小组”实施攻击后给三家游戏公司发的邮件。二是做好犯罪嫌疑人线上身份和线下身份同一性的认定工作，并查清“暗夜小组”各成员在犯罪中的分工、地位和作用。三是查清犯罪行为造成的危害后果。

（二）审查起诉

2017年9月19日，公安机关将案件移送广东省深圳市南山区人民检察院审查起诉。鉴于在案证据已基本厘清“暗夜小组”实施犯罪的脉络，“暗夜小组”成员的认罪态度开始有了转变。经审查，全案基本事实已经查清，基本证据已经调取，能够认定姚晓杰等人的行为已涉嫌破坏计算机信息系统罪：一是可以认定系“暗夜小组”对某互联网公司云服务器实施了大流量攻击。国家计算机网络应急技术处理协调中心广东分中心出具的报告证实，筛选出的大流量攻击源IP中有198个IP为僵尸网络中的被控主机，这些主机由14个控制端服务器控制。通过比对丁虎子等人电脑中的电子数据，证实丁虎子等人控制的服务器就是对三家游戏公司客户端实施网络攻击的服务器。分析报告还明确了云服务器受到的攻击类型和攻击采用的网络协议、波形特征，这些证据与“暗夜小组”成员供述的攻击资源特征一致。网络聊天内容和银行交易流水等证据证实“暗夜小组”向丁虎子等三人购买上述14个控制端服务器控制权的事实。电子邮件等证据进一步印证了“暗夜小组”实施攻击的事实。二是通过进一步提取犯罪嫌疑人网络活动记录、犯罪嫌疑人之间的通讯信息、资金往来等证据，结合对电子数据的分析，查清了“暗夜小组”成员虚拟身份与真实身份的对应关系，查明了小组成员在招募人员、日常管理、购买控制端服务器、实施攻击和后勤等各个环节中的分工负责情况。

审查中，检察机关发现，攻击行为造成的损失仍未查清：部分犯罪嫌疑人实施犯罪的次数，上下游间交易的证据仍欠缺。针对存在的问题，深圳市南山区人民检察院与公安机关进行了积极沟通，于2017年11月2日和2018年1月16日两次将案件退回公安机关补充侦查。一是鉴于证实受影响计算机信息系统和用户数量的证据已无法调取，本案只能以造成的经济损失认定危害后果。因此要求公安机关补充调取能够证实某互联网公司直接经济损失或为恢复网络正常运行支出的必要费用等证据，并交专门机构作出评估。二是进一步补充证实“暗夜小组”成员参与每次网络攻击具体情况以及攻击服务器控制权在“暗夜小组”与丁虎子等人间流转情况的证据。三是对丁虎子等人向“暗夜小组”提供攻击服务器控制权的主观明知证据作进一步补强。

公安机关按要求对证据作了补强和完善，全案事实已查清，案件证据确实充分，已经形成了完整的证据链条。

（三）出庭指控犯罪

2018年3月6日，深圳市南山区人民检察院以被告人姚晓杰等11人构成破坏计算机信息系统罪向深圳市南山区人民法院提起公诉。4月27日，法院公开开庭审理了本案。

庭审中，11名被告人对检察机关的指控均表示无异议。部分辩护人提出以下辩护意见：一是网络攻击无处不在，现有证据不能认定三家网络游戏公司受到的攻击均是“暗夜小组”发动的，不能排除攻击来自其他方面。二是即便认定“暗夜小组”参与对三家网络游戏公司的攻击，也不能将某互联网公司支付给抢修系统数据的员工工资认定为本案的经济损失。

针对辩护意见，公诉人答辩如下：一是案发时并不存在其他大规模网络攻击，在案证据足以证实只有“暗夜小组”针对云服务器进行了DDoS高流量攻击，每次的攻击时间和被攻击的时间完全吻合，攻击手法、流量波形、攻击源IP和攻击路径与被告人供述及其他证据相互印证，现有证据足以证明三家网络游戏公司客户端不能正常运行系受“暗夜小组”攻击导致。二是根据法律规定，“经济损失”包括危害计算机信息系统犯罪行为给用户直接造成的经济损失以及用户为恢复数据、功能而支出的必要费用。某互联网公司为修复系统数据、功能而支出的员工工资系因犯罪产生的必要费用，应当认定为本案的经济损失。

（四）处理结果

2018年6月8日，广东省深圳市南山区人民法院判决认定被告人姚晓杰等11人犯破坏计算机信息系统罪；鉴于各被告人均表示认罪悔罪，部分被告人具有自首等法定从轻、减轻处罚情节，对11名被告人分别判处有期徒刑一年至二年不等。宣判后，11名被告人均未提出上诉，判决已生效。

**【指导意义】**

（一）立足网络攻击犯罪案件特点引导公安机关收集调取证据。对重大、疑难、复杂的网络攻击类犯罪案件，检察机关可以适时介入侦查引导取证，会同公安机关研究侦查方向，在收集、固定证据等方面提出法律意见。一是引导公安机关及时调取证明网络攻击犯罪发生、证明危害后果达到追诉标准的证据。委托专业技术人员对收集提取到的电子数据等进行检验、鉴定，结合在案其他证据，明确网络攻击类型、攻击特点和攻击后果。二是引导公安机关调取证明网络攻击是犯罪嫌疑人实施的证据。借助专门技术对攻击源进行分析，溯源网络犯罪路径。审查认定犯罪嫌疑人网络身份与现实身份的同一性时，可通过核查IP地址、网络活动记录、上网终端归属，以及证实犯罪嫌疑人与网络终端、存储介质间的关联性综合判断。犯罪嫌疑人在实施网络攻击后，威胁被害人的证据可作为认定攻击事实和因果关系的证据。有证据证明犯罪嫌疑人实施了攻击行为，网络攻击类型和特点与犯罪嫌疑人实施的攻击一致，攻击时间和被攻击时间吻合的，可以认定网络攻击系犯罪嫌疑人实施。三是网络攻击类犯罪多为共同犯罪，应重点审查各犯罪嫌疑人的供述和辩解、手机通信记录等，通过审查自供和互证的情况以及与其他证据间的印证情况，查明各犯罪嫌疑人间的犯意联络、分工和作用，准确认定主、从犯。四是对需要通过退回补充侦查进一步完善上述证据的，在提出补充侦查意见时，应明确列出每一项证据的补侦目的，以及为了达到目的需要开展的工作。在补充侦查过程中，要适时与公安机关面对面会商，了解和掌握补充侦查工作的进展，共同研究分析补充到的证据是否符合起诉和审判的标准和要求，为补充侦查工作提供必要的引导和指导。

（二）对被害单位提供的证据和技术支持意见需结合其他在案证据作出准确认定。网络攻击类犯罪案件的被害人多为大型互联网企业。在打击该类犯罪的过程中，司法机关往往会借助被攻击的互联网企业在网络技术、网络资源和大数据等方面的优势，进行溯源分析或对攻击造成的危害进行评估。由于互联网企业既是受害方，有时也是技术支持协助方，为确保被害单位提供的证据客观真实，必须特别注意审查取证过程的规范性；有条件的，应当聘请专门机构对证据的完整性进行鉴定。如条件不具备，应当要求提供证据的被害单位对证据作出说明。同时要充分运用印证分析审查思路，将被害单位提供的证据与在案其他证据，如从犯罪嫌疑人处提取的电子数据、社交软件聊天记录、银行流水、第三方机构出具的鉴定意见、证人证言、犯罪嫌疑人供述等证据作对照分析，确保不存在人为改变案件事实或改变案件危害后果的情形。

（三）对破坏计算机信息系统的危害后果应作客观全面准确认定。实践中，往往倾向于依据犯罪违法所得数额或造成的经济损失认定破坏计算机信息系统罪的危害后果。但是在一些案件中，违法所得或经济损失并不能全面、准确反映出犯罪行为所造成的危害。有的案件违法所得或者经济损失的数额并不大，但网络攻击行为导致受影响的用户数量特别大，有的导致用户满意度降低或用户流失，有的造成了恶劣社会影响。对这类案件，如果仅根据违法所得或经济损失数额来评估危害后果，可能会导致罪刑不相适应。因此，在办理破坏计算机信息系统犯罪案件时，检察机关应发挥好介入侦查引导取证的作用，及时引导公安机关按照法律规定，从扰乱公共秩序的角度，收集、固定能够证实受影响的计算机信息系统数量或用户数量、受影响或被攻击的计算机信息系统不能正常运行的累计时间、对被害企业造成的影响等证据，对危害后果作出客观、全面、准确认定，做到罪责相当、罚当其罪，使被告人受到应有惩处。

**【相关规定】**

《中华人民共和国刑法》第二百八十六条

《最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》第四条、第六条、第十一条