破坏计算机信息系统罪的解释学研究之法律检索指南

【作者简介】张琼辉，浙江大学光华法学院 2017 级刑法学科硕

【指导教师】罗伟博士，美国华盛顿大学法学院

第一部分　破坏计算机信息系统罪的解释学研究论题的提出背景

自 1997 年增设破坏计算机信息系统罪以来，此类判决的数量逐年呈上升趋势，特别是 2013 年以后增长速度较快。到 2018 年 5 月 20 日，中国国裁判文书网上有关破坏计算机信息系统的判决共有 458 个，且多分布于上海、浙江、广东等沿海发达地区。随着互联网技术的发展，新型网络犯罪层出不穷，面对新型犯罪方式，破坏计算机信息系统罪出现了同案不同判的现象。

根据《刑法》法条中的规定，可以认定为“破坏计算机信息系统罪”的行为有以下三种：一是违反国家规定，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，后果严重的；二是违反国家规定，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，后果严重的；三是故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的。

《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》第四条对以上三种行为分别做出了更为具体的解释：破坏计算机信息系统功能、数据或者应用程序，具有下列情形之一的，应当认定为刑法第二百八十六条第一款和第二款规定的“后果严重”：（一）造成十台以上计算机信息系统的主要软件或者硬件不能正常运行的；（二）对二十台以上计算机信息系统中存储、处理或者传输的数据进行删除、修改、增加操作的；（三）

违法所得五千元以上或者造成经济损失一万元以上的；（四）造成为一百台以上计算机信息系统提供域名解析、身份认证、计费等基础服务或者为一万以上用户提供服务的计算机信息系统不能正常运行累计一小时以上的；（五）造成其他严重后果的。此外，根据第五条“计算机病毒等破坏性程序”：（一）能够通过网络、存储介质、文件等媒介，将自身的部分、全部或者变种进行复制、传播，并破坏计算机系统功能、数据或者应用程序的；（二）能够在预先设定条件下自动触发，并破坏计算机系统功能、数据或者应用程序的；（三）其他专门设计用于破坏计算机系统功能、数据或者应用程序的程序。

通过整理上述条文和司法解释，笔者发现，实务中对“破坏”界定不清晰的根本原因，是现有的法条对“破坏”行为的规定模糊，司法解释也没有对“删除”“修改”、“干扰”、“后果严重”、“正常运行”做出进一步明确的解释，导致司法实践中审判人员理解的差异。这不仅极大了影响了该罪名的准确适用，也会造成该罪名的泛化风险。因此，笔者在分析“流量劫持”的案件时，将通过对现有观点的梳理，分析“流量劫持”的是否可以解释成“破坏”行为，并且结合笔者的实证研究，进一步对破坏计算机信息系统罪的“破坏”行为开展研究。

第二部分 破坏计算机信息系统罪的解释学研究之文献检索指南概述

一、5W 分析法

- who：网站运营者（website operators）、计算机信息系统（Computer Information System）、计算机犯罪（cybercrime or Computer hackers）
- what：破坏计算机信息系统罪在司法适用上存在差异、破坏（destroy, hacking, tampering）、滥用（misuse）

- where：网络空间（cyberspace）
- when：司法适用（jurisdiction）
- why：“破坏行为”（scope of damage）界限模糊

二、关键词

破坏（Destroy）、侵入（Invade or hack）、计算机信息系统（Computer Information System）、滥用（Misuse or tampering）

三、检索词

破坏 （Destroy or hack）、计算机信息系统（Computer Information System）、滥用 （Misuse）、破坏（destroy）

四、检索工具

- 中国检索网站：北大法宝，中国知网，威科先行
- 国外检索网站：Westlaw，Lexis，Heinonline

第三部分 文献检索之中文一次资源与二次资源

一、 中文一次资源

- **现行法律**

选用数据库：威科先行

检索步骤：法律法规-全文-精确搜索，在检索框中输入“破坏计算机信息系统”

检索结果：法律 3 篇，如下：

（1）2017 年《中华人民共和国刑法》第 286 条（载“威科先行”）

【破坏计算机信息系统罪】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，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。

违反国家规定，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，后果严重的，依照前款的规定处罚。

故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。

单位犯前三款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照第一款的规定处罚。

（2）2012 年《中华人民共和国治安管理处罚法》第 29 条

第二十九条有下列行为之一的，处五日以下拘留；情节较重的，处五日以上十日以下拘留：

（一）违反国家规定，侵入计算机信息系统，造成危害的；

（二）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的；

（三）违反国家规定，对计算机信息系统中存储、处理、传输的数据和应用程序进行删除、修改、增加的；

（四）故意制作、传播计算机病毒等破坏性程序，影响计算机信息系统正常运行的。

（3）1997 年《中华人民共和国刑法》第 286 条

第二百八十六条违反国家规定，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，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。

违反国家规定，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，后果严重的，依照前款的规定处罚。

故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。

- **行政法规**

选用数据库：威科先行

检索步骤：法律法规-全文-精确搜索，在检索框中输入“破坏计算机信息系统”

检索结果：行政法规 4 篇，经筛选

（1）2016 年《互联网上网服务营业场所管理条例》第 15 条

第十五　条互联网上网服务营业场所经营单位和上网消费者不得进行下列危害信息网络安全的活动：

(一)故意制作或者传播计算机病毒以及其他破坏性程序的；

(二)非法侵入计算机信息系统或者破坏计算机信息系统功能、数据和应用程序的；

(三)进行法律、行政法规禁止的其他活动的。

- **最高人民法院司法解释及文件**

选用数据库：威科先行

检索步骤：法律法规-全文-精确搜索，在检索框中输入“破坏计算机信息系统”

检索结果：司法解释及文件 6 篇，经筛选


司法解释/文件（6）

1 最高人民法院、最高人民检察院关于办理环境污染刑事案件适用法律若干问题的解释（2016）
[最高人民法院,最高人民检察院] [法释〔2016〕29号] [2016.12.23 发布] [2017.01.01 实施] [中英对照] [English]
【官方解读】【专家解读】
摘要： 施下列行为，或者强令、指使、授意他人实施下列行为的，应当依照刑法第二百八十六条的规定，以破坏计算机信息系统罪论处： （一）修改参数或者监测数据的； （二）干扰采样，致使监测数据严重失...

2 最高人民法院关于充分发挥审判职能作用切实维护公共安全的若干意见
[最高人民法院] [法发〔2015〕12号] [2015.09.16 发布] [2015.09.16 实施]
摘要： 、破坏计算机信息系统以及制作、销售、使用“伪基站”设备等犯罪活动，从严惩治针对基础信息网络、重要行业和领域的重要信息系统、军事网络、重要政务网络、用户数量众多的商业网络的攻击破坏活动，从严惩治利用攻击破坏...

3 最高人民法院、最高人民检察院、公安部、国家安全部关于依法办理非法生产销售使用 “伪基站”设备案件的意见
[最高人民法院,最高人民检察院,公安部,国家安全部] [公通字〔2014〕13号] [2014.03.14 发布] [2014.03.14 实施]
摘要： 基站”设备干扰公用电信网络信号，危害公共安全的，依照《刑法》第一百二十四条第一款的规定，以破坏公用电信设施罪追究刑事责任；同时构成虚假广告罪、非法获取公民个人信息罪、破坏计算机信息系统罪、扰乱无线电通讯...

4 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
[最高人民法院,最高人民检察院] [法释〔2011〕19号] [2011.08.01 发布] [2011.09.01 实施] [中英对照] [English]
摘要： ； （二）其他情节特别严重的情形。 第四条 破坏计算机信息系统功能、数据或者应用程序，具有下列情形之一的，应当认定为刑法第二百八十六条第一款和第二款规定的“后果严重”： （一）造成十台...

5 关于印发《最高人民检察院关于适用刑法分则规定的犯罪的罪名的意见》的通知
[最高人民检察院] [高检发释字〔1997〕3号] [1997.12.25 发布] [1997.12.25 实施]
摘要： 间谍专用器材罪（第２８３条） ２０９、非法使用窃听、窃照专用器材罪（第２８４条） ２１０、非法侵入计算机信息系统罪（第２８５条） ２１１、破坏计算机信息系统罪（第２８６条） ２１２、扰乱无线电通...

6 最高人民法院关于执行《中华人民共和国刑法》确定罪名的规定
[最高人民法院] [法释〔1997〕〕9号] [1997.12.11 发布] [1997.12.16 实施]
摘要： ２８３条 非法生产、销售间谍专用器材罪 第２８４条 非法使用窃听、窃照专用器材罪 第２８５条 非法侵入计算机信息系统罪 第２８６条 破坏计算机信息系统罪 第２８８条...

（1）2016 年《最高人民法院、最高人民检察院关于办理环境污染刑事案件适用法律若干问题的解释》第 10 条

第十条违反国家规定，针对环境质量监测系统实施下列行为，或者强令、指使、授意他人实施下列行为的，应当依照刑法第二百八十六条的规定，以破坏计算机信息系统罪论处：

（一）修改参数或者监测数据的；

（二）干扰采样，致使监测数据严重失真的；

（三）其他破坏环境质量监测系统的行为。

重点排污单位篡改、伪造自动监测数据或者干扰自动监测设施，排放化学需氧量、氨氮、二氧化硫、氮氧化物等污染物，同时构成污染环境罪和破坏计算机信息系统罪的，依照处罚较重的规定定罪处罚。

从事环境监测设施维护、运营的人员实施或者参与实施篡改、伪造自动监测数据、干扰自动监测设施、破坏环境质量监测系统等行为的，应当从重处罚。

（2）2015 年《最高人民法院关于充分发挥审判职能作用切实维护公共安全的若干意见》第 14 条

依法惩治网络攻击破坏犯罪。信息时代，网络已深度融入经济社会的各个方面，网络安全已成为公共安全的重要组成部分，与广大人民群众的信息安全、财产安全乃至人身安全密切相关。要依法打击非法侵入、破坏计算机信息系统以及制作、销售、使用“伪基站”设备等犯罪活动，从严惩治针对基础信息网络、重要行业和领域的重要信息系统、军事网络、重要政务网络、用户数量众多的商业网络的攻击破坏活动，从严惩治利用攻击破坏非法获取国家秘密、商业秘密、公民个人信息等犯罪活动。

（3）2011 年《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》

第四条破坏计算机信息系统功能、数据或者应用程序，具有下列情形之一的，应当认定为刑法第二百八十六条第一款和第二款规定的“后果严重”：

（一）造成十台以上计算机信息系统的主要软件或者硬件不能正常运行的；

（二）对二十台以上计算机信息系统中存储、处理或者传输的数据进行删除、修改、增加操作的；

（三）违法所得五千元以上或者造成经济损失一万元以上的；

（四）造成为一百台以上计算机信息系统提供域名解析、身份认证、计费等基础服务或者为一万以上用户提供服务的计算机信息系统不能正常运行累计一小时以上的；

（五）造成其他严重后果的。

实施前款规定行为，具有下列情形之一的，应当认定为破坏计算机信息系统“后果特别严重”：

（一）数量或者数额达到前款第（一）项至第（三）项规定标准五倍以上的；

（二）造成为五百台以上计算机信息系统提供域名解析、身份认证、计费等基础服务或者为五万以上用户提供服务的计算机信息系统不能正常运行累计一小时以上的；

（三）破坏国家机关或者金融、电信、交通、教育、医疗、能源等领域提供公共服务的计算机信息系统的功能、数据或者应用程序，致使生产、生活受到严重影响或者造成恶劣社会影响的；

（四）造成其他特别严重后果的。

第六条故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，具有下列情形之一的，应当认定为刑法第二百八十六条第三款规定的“后果严重”：

（一）制作、提供、传输第五条第（一）项规定的程序，导致该程序通过网络、存储介质、文件等媒介传播的；

（二）造成二十台以上计算机系统被植入第五条第（二）、（三）项规定的程序的；

（三）提供计算机病毒等破坏性程序十人次以上的；

（四）违法所得五千元以上或者造成经济损失一万元以上的；

（五）造成其他严重后果的。

实施前款规定行为，具有下列情形之一的，应当认定为破坏计算机信息系统“后果特别严重”：

（一）制作、提供、传输第五条第（一）项规定的程序，导致该程序通过网络、存储介质、文件等媒介传播，致使生产、生活受到严重影响或者造成恶劣社会影响的；

（二）数量或者数额达到前款第（二）项至第（四）项规定标准五倍以上的；

（三）造成其他特别严重后果的。

- **案例、裁判文书**

选用数据库：中国国裁判文书网

检索步骤：司法案例-刑事，在检索框中输入“破坏计算机信息系统罪”

检索结果：指导性案例 3 篇，公报案例 5 篇，典型案例 1 篇，参阅案例 3 篇，经典案例 50 篇，法宝推荐 151 篇，普通案例 598 篇。经筛选：

（1） 指导性案例

1.检例第35号：曾兴亮、王玉生破坏计算机信息系统、敲诈案

案情简介：2016年10月至11月，被告人曾兴亮与王玉生结伙或者单独使用聊天社交软件，冒充年轻女性与被害人聊天，谎称自己的苹果手机因故障无法登录“iCloud”（云存储），请被害人代为登录，诱骗被害人先注销其苹果手机上原有的ID，再使用被告人提供的ID及密码登录。随后，曾、王二人立即在电脑上使用新的ID及密码登录苹果官方网站，利用苹果手机相关功能将被害人的手机设置修改，并使用“密码保护问题”修改该ID的密码，从而远程锁定被害人的苹果手机。曾、王二人再在其个人电脑上，用网络聊天软件与被害人联系，以解锁为条件索要钱财。采用这种方式，曾兴亮单独或合伙作案共21起，涉及苹果手机22部，锁定苹果手机21部，索得人民币合计7290元；王玉生参与作案12起，涉及苹果手机12部，锁定苹果手机11部，索得人民币合计4750元。2016年11月24日，二人被公安机关抓获。

2.检例第34号：李骏杰等破坏计算机信息系统案

2011年5月至2012年12月，被告人李骏杰在工作单位及自己家中，单独或伙同他人通过聊天软件联系需要修改中差评的某购物网站卖家，并从被告人黄福权等处购买发表中差评的该购物网站买家信息300余条。李骏杰冒用买家身份，骗取客服审核通过后重置账号密码，登录该购物网站内部评价系统，删改买家的中差评347个，获利9万余元。

3. 检例第33号：李丙龙破坏计算机信息系统案

被告人李丙龙为牟取非法利益，预谋以修改大型互联网网站域名解析指向的方法，劫持互联网流量访问相关赌博网站，获取境外赌博网站广告推广流量提成。2014年10月20日，李丙龙冒充某知名网站工作人员，采取伪造该网站公司营业执照

等方式，骗取该网站注册服务提供商信任，获取网站域名解析服务管理权限。10月21日，李丙龙通过其在域名解析服务网站平台注册的账号，利用该平台相关功能自动生成了该知名网站二级子域名部分DNS（域名系统）解析列表，修改该网站子域名的IP指向，使其连接至自己租用境外虚拟服务器建立的赌博网站广告发布页面。当日19时许，李丙龙对该网站域名解析服务器指向的修改生效，致使该网站不能正常运行。23时许，该知名网站经技术排查恢复了网站正常运行。11月25日，李丙龙被公安机关抓获。至案发时，李丙龙未及获利。

经司法鉴定，该知名网站共有559万有效用户，其中邮箱系统有36万有效用户。按日均电脑客户端访问量计算，10月7日至10月20日邮箱系统日均访问量达12.3万。李丙龙的行为造成该知名网站10月21日19时至23时长达四小时左右无法正常发挥其服务功能，案发当日仅邮件系统电脑客户端访问量就从12.3万减少至4.43万。

二、中文二次文献

- **中文著作**

选用数据库：浙江大学光华法学院“我的图书馆”

检索步骤：所有字段-多库检索-刑法，搜索关键词“网络”“犯罪”，经筛选：

（1）季境.《新型网络犯罪研究》.2012年

内容简介：从刑法理论和犯罪学角度，对目前网络环境中各种危害社会的行为，特别是新型网络犯罪行为进行了系统的分析研究，并有针对性地提出了防控对策，最后对网络犯罪电子证据的获取和应用进行了有益的探讨。

（2）皮勇.《网络犯罪比较研究》.2005年

内容简介：该书通过比较研究的方法，在分析和比较各国有关刑法制度的基础上，在网络犯罪方面为我国的刑法立法完善提供可靠的理论依据。

- **中文期刊**

选用数据库：中国知网

关键词：破坏计算机信息系统罪、流量劫持

（1）俞小海.《破坏计算机信息系统罪之司法实践分析与规范含义重构》[J].交大法学,2015 年(03).

通过对 43 个相关司法判例的梳理和分析,得出破坏计算机信息系统罪司法实践中存在数罪并罚问题认定不一、类似行为评价差异较大、"后果严重"认定模糊、适用范围过度扩张等问题。实践中,通过降低"后果严重"的标准和扩大对计算机信息系统数据之解释,使得破坏计算机信息系统罪具有极强的适用力,呈现"口袋化"之趋势,偏离了破坏计算机信息系统罪的文本含义和规范构造。为此,应当将本罪"后果严重"限定为与计算机信息系统安全具有关联性的后果,将计算机信息系统数据限缩为核心数据和核心应用程序,在此基础上准确认定利用计算机实施犯罪的罪数形态。

（2）叶良芳.《刑法教义学视角下流量劫持行为的性质研究》[J].中州法学,2016,(08).

流量劫持是强制用户访问某些网站或网页的行为,根据对用户上网自主权侵犯程度的不同,可以将其划分为域名劫持和链路劫持两种类型。域名劫持行为通过修改用户计算机信息系统的数据,使用户不能访问目标网站或网页,既触犯了非法控制计算机信息系统罪,又触犯了破坏计算机信息系统罪,应按想象竞合犯的处断原则,以破坏计算机信息系统罪论处。链路劫持行为仅对用户上网造成一

定的干扰,法益侵害程度较低且不能充足相关犯罪的构成要件,因而不应以犯罪论处。但这种行为侵犯了网络服务提供商的公平竞争利益,构成不正当竞争。

（3）徐光华.“以刑制罪”视阈下财产罪保护法益的再认识[J].中国法学,2016(06).

对 81 个"非法取回本人所有而被他人合法占有的财物"样本案例的定罪、量刑、犯罪数额认定的考察发现,原则上只有造成占有人财产损失的才会以财产罪定罪,而若判处财产罪会导致量刑畸重,所以,样本判决限制财产罪的适用和犯罪数额的认定以实现量刑轻缓。本文认为,优先考虑量刑合理的"以刑制罪"忽略了定罪的准确性,易消弥财产罪之间、财产罪与其他罪之间的界限;部分判决量刑畸轻、犯罪数额认定混乱、判决书说理不一;样本判决"以刑制罪"有其实践理性,但缺乏必要的规范约束易导致乱象。由此反思我国刑法对财产罪的定量立法模式,较重的法定刑是导致"以刑制罪"的根本原因。立法赋予量刑更大的裁量空间将有助于缓解司法上的"以刑制罪",也有助于对包括占有权在内的财产法益的全面保护并实现罪刑均衡。

（4）于志刚.口袋罪的时代变迁、当前乱象与消减思路[J].法学家,2013,(03).

（5）谭宇.刑法学视域下侵害网络流量问题研究[J].太原理工大学学报（社会科学版）,2016,(03).

（6）陈成伟.破坏计算机信息系统罪行为方式之辨析[J].法制博览（法律实务）,2018 年(04).

（7)姜瀛.口袋思维——入侵网络犯罪的不当倾向及其应对进路[J].苏州大学学报（法学版）,2017,(02).

（8）孙道萃.流量劫持的刑法规制及完善[J].中国检察官,2016(04).

（9）朱赫，孙国祥，刘艳红，桂万先，卜向敏，杨赞，马健，张永健.破坏计算机信息系统案件法律适用探讨[J].人民检察,2015(08).

（10）谭宇.刑法学视域下侵害网络流量问题研究[J].太原理工大学学报（社会科学版）,2016(03).

……

第四部分 文献检索之外文一次资源与二次资源

一、外文一次资源

- **Federal（美国联邦法）**

选用数据库：westlaw –USCA

关键词：“computer system”“destroy”“hack”

检索步骤：选择 USCA-输入"information system" or "computer system" 5/ destroy,

显示 41 个结果，经筛选：

1. **Title 34. Crime Control and Law Enforcement (Refs & Annos) 第 30101 条，**

To be eligible to receive a grant under this section, a State shall provide assurances to the Attorney General that the State--

(1) has in effect laws that penalize computer crime, such as criminal laws prohibiting--

(A) fraudulent schemes executed by means of a computer system or network;

(B) the unlawful damaging, destroying, altering, deleting, removing of computer software, or data contained in a computer, computer system, computer program, or computer network; or

(C) the unlawful interference with the operation of or denial of access to a computer, computer program, computer system, or computer network;

翻译如下：为了有资格根据本节获得赠款，一国应向检察总长保证，国 -

（1）实际上是惩罚计算机犯罪的法律，例如禁止 -

（A）通过计算机系统或网络执行的欺诈计划;

（B）计算机，计算机系统，计算机程序或计算机网络中包含的非法破坏，破坏，更改，删除，删除计算机软件或数据;要么

（C）非法干扰操作或拒绝访问计算机，计算机程序，计算机系统或计算机网络;

2. Computer Fraud and Abuse Act

Criminal offenses under the Act:

(a) Whoever—

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national

defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602 (n) [1] of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

(5)

(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States;

a）无论是谁

（1）在未经授权的情况下故意访问计算机或以其他方式授权访问计算机，并通过该计算机获取计算机第 y 段中定义的辩护或外交关系或任何受限制的数据。

1954 年“原子能法”第 11 条，有理由相信这些信息可能会或可能不会传递到美国沟通，交付，传播，交付，传达，交付，传播，交付或传播，或故意保留，并未能交付给官员或美国雇员有权获得;

（2）未经授权故意访问计算机

标题 15 的 1602（n）[1]，或作为搜索，包含在消费者的消费者报告机构的文件中术语在“公平信用法”中定义;

（B）来自美国任何部门或机构的信息;或

（C）来自任何受保护计算机的信息;

（3）在未经授权的情况下，未经授权访问访问美国或美利坚合众国的美国机构或部门的任何非公用计算机，不是专门用于此类用途的计算机，由美国政府使用或由美国政府使用;

（4）明知并意图诈骗，访问受保护的计算机没有授权或超出授权的访问，并寻求行为的手段进一步加强有意诈骗，并获得任何有价值的东西，除非造假的对象和东西获得 besteht 只任何 1 年期间$ 5,000;

（5）

（A）故意导致程序，信息，代码或命令的传输，并且由于此类行为，故意在未经授权的情况下对受保护的计算机造成损害;

（B）未经授权故意访问受保护的计算机，并且由于此类行为，不计后地造成损害;或

（C）未经授权故意访问受保护的计算机，并且由于搜索行为，导致损坏和丢失。

（6）故意及故意以任何密码欺骗交易（定义见第 1029 条）

（A）此类贩运影响州际贸易或外国贸易;或

（B）此类计算机由美国政府使用或由美国政府使用;

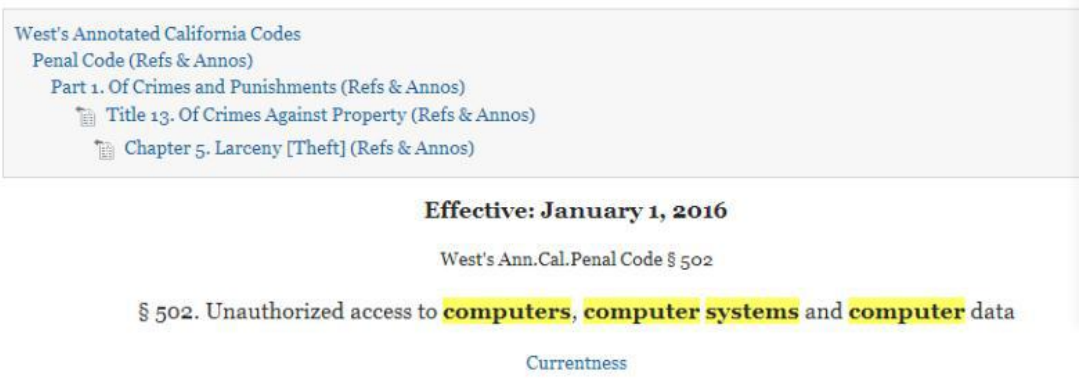
- **State Statues（加利福尼亚州的法律条文）**

选用数据库：westlaw

关键词：“computer system”“information system”“destroy”

检索步骤：选择 California——输入“computer system”or “information system”5/ destroy，选择 states，显示 44 个结果，经筛选：

（1）第 502 条



：(a) It is the intent of the Legislature in enacting this section to expand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems. The Legislature finds and declares that the proliferation of computer technology has resulted in a concomitant proliferation of computer crime and other forms of unauthorized access to computers, computer systems, and computer data.

The Legislature further finds and declares that protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals as well as to the well-being of

financial institutions, business concerns, governmental agencies, and others within this state that lawfully utilize those computers, computer systems, and data.

(b) For the purposes of this section, the following terms have the following meanings:

(1) “Access” means to gain entry to, instruct, cause input to, cause output from, cause data processing with, or communicate with, the logical, arithmetical, or memory function resources of a computer, computer system, or computer network.

(2) “Computer network” means any system that provides communications between one or more computer systems and input/output devices, including, but not limited to, display terminals, remote systems, mobile devices, and printers connected by telecommunication facilities.

(3) “Computer program or software” means a set of instructions or statements, and related data, that when executed in actual or modified form, cause a computer, computer system, or computer network to perform specified functions.

(4) “Computer services” includes, but is not limited to, computer time, data processing, or storage functions, Internet services, electronic mail services, electronic message services, or other uses of a computer, computer system, or computer network.

(5) “Computer system” means a device or collection of devices, including support devices and excluding calculators that are not programmable and capable of being used in conjunction with external files, one or more of which contain computer programs, electronic instructions, input data, and output data, that performs functions,

including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control.

(6) “Government computer system” means any computer system, or part thereof, that is owned, operated, or used by any federal, state, or local governmental entity.

(7) “Public safety infrastructure computer system” means any computer system, or part thereof, that is necessary for the health and safety of the public including computer systems owned, operated, or used by drinking water and wastewater treatment facilities, hospitals, emergency service providers, telecommunication companies, and gas and electric utility companies.

(8) “Data” means a representation of information, knowledge, facts, concepts, computer software, or computer programs or instructions. Data may be in any form, in storage media, or as stored in the memory of the computer or in transit or presented on a display device.

(9) “Supporting documentation” includes, but is not limited to, all information, in any form, pertaining to the design, construction, classification, implementation, use, or modification of a computer, computer system, computer network, computer program, or computer software, which information is not generally available to the public and is necessary for the operation of a computer, computer system, computer network, computer program, or computer software.

(10) “Injury” means any alteration, deletion, damage, or destruction of a computer system, computer network, computer program, or data caused by the access, or the denial of access to legitimate users of a computer system, network, or program.

(11) “Victim expenditure” means any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, deleted, damaged, or destroyed by the access.

(12) “Computer contaminant” means any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. They include, but are not limited to, a group of computer instructions commonly called viruses or worms, that are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources, modify, destroy, record, or transmit data, or in some other fashion usurp the normal operation of the computer, computer system, or computer network.

翻译如下：（a）立法机构制定本节的目的是扩大对个人，企业和政府机构的保护程度，使其免受篡改，干扰，破坏和未经授权访问合法创建的计算机数据和计算机系统。立法机构认定并宣称计算机技术的扩散导致计算机犯罪和其他形式的未授权访问计算机，计算机系统和计算机数据的同时泛滥。

立法机构进一步认定并声明，保护所有类型和形式的合法创建的计算机，计算机系统和计算机数据的完整性对于保护个人隐私以及保护金融机构，企业的福利至关重要担忧，政府机构以及该州的其他机构合法使用这些计算机，计算机系统和数据。

（b）就本节而言，以下术语具有以下含义：

（1）“访问”是指进入，指示，引起输入，引起输出，引起数据处理，或与计算机，计算机系统或计算机网络的逻辑，算术或存储器功能资源通信。

（2）“计算机网络”是指在一个或多个计算机系统和输入/输出设备之间提供通信的任何系统，包括但不限于通过电信设施连接的显示终端，远程系统，移动设备和打印机。

（3）“计算机程序或软件”是指当以实际或修改形式执行时使计算机，计算机系统或计算机网络执行指定功能的一组指令或语句以及相关数据。

（4）“计算机服务”包括但不限于计算机时间，数据处理或存储功能，互联网服务，电子邮件服务，电子信息服务或计算机，计算机系统或计算机网络的其他用途。

（5）“计算机系统”是指包括支持设备在内的设备或设备集合，不包括不可编程且能够与外部文件结合使用的计算器，其中一个或多个文件包含计算机程序，电子指令，输入数据以及执行功能的输出数据，包括但不限于逻辑，算术，数据存储和检索，通信和控制。

（6）“政府计算机系统”是指任何联邦，州或地方政府实体拥有，操作或使用的任何计算机系统或其部分。

（7）“公共安全基础设施计算机系统”是指公众健康和安全所必需的任何计算机系统或其部分，包括饮用水和废水处理设施，医院，紧急事件所拥有，操作或使用的计算机系统服务提供商，电信公司以及燃气和电力公司。

（8）“数据”是指信息，知识，事实，概念，计算机软件或计算机程序或指令的表示。数据可以以任何形式，在存储介质中，或者存储在计算机的存储器中或在传送中或呈现在显示设备上。

（9）“支持文件”包括但不限于与计算机，计算机系统，计算机网络，计算机程序等的设计，构造，分类，实施，使用或修改有关的任何形式的所有信息。或计算机软件，该信息通常不是公众可获得的，并且是计算机，计算机系统，计算机网络，计算机程序或计算机软件的操作所必需的。

（10）“损害”是指因访问或拒绝访问计算机系统，网络的合法用户而导致的计算机系统，计算机网络，计算机程序或数据的任何更改，删除，损坏或破坏，或程序。

（11）“受害者支出”是指业主或承租人为验证计算机系统，计算机网络，计算机程序或数据是否被更改，删除，损坏或通过访问而遭到破坏而合理地发生的任何支出。

（12）“计算机污染物”是指任何旨在修改，损坏，破坏，记录或传输计算机，计算机系统或计算机网络内的信息的计算机指令集，而无意信息所有者的意图或许可。它们包括但不限于一组通常称为病毒或蠕虫的计算机指令，这些指令是自我复制或自我繁殖的，并且被设计为污染其他计算机程序或计算机数据，消耗计算机资源，修改，销毁，记录，或传输数据，或以某种其他方式篡夺计算机，计算机系统或计算机网络的正常运行。

- **判例（Cases）**

（1）NovelPoster v. Javitch Canfield Group, et al. Case No. 13–cv–05186–WHO. Signed November 03, 2014

This case involves the soured relationship between the owners of the plaintiff company, NovelPoster, and the defendant company engaged to operate it, Javitch

Canfield Group. Javitch Canfield Group's owners, Mark Javitch and Daniel Canfield, are also defendants. NovelPoster asserts various causes of action under both federal and state law based on the defendants' allegedly unlawful access of NovelPoster's email and other electronic accounts during the start, breakdown, and wake of the parties' relationship.

The defendants filed this limited Motion for Judgment on the Pleadings, arguing that NovelPoster's allegations as pleaded in the Complaint fail to support the First through Fourth Causes of Action for violations of the federal Computer Fraud and Abuse Act, the federal Electronic Communications Privacy Act, California's Comprehensive Computer Data Access and Fraud Act, and California's Invasion of Privacy Act. The motion is GRANTED. NovelPoster fails to adequately plead loss to support its causes of action under the Computer Fraud and Abuse Act and California's *940 Comprehensive Computer Data Access and Fraud Act and fails to plead that the defendants “intercepted” any electronic communications under the Electronic Communications Privacy Act and California's Invasion of Privacy Act.

这起案件涉及原告公司 NovelPoster 与参与经营的被告公司 Javitch Canfield Group， Javitch Canfield 集团的所有者 Mark Javitch 和 Daniel Canfield 也作为被告。 NovelPoster 根据联邦和州法律提出各种诉讼理由，其依据是被告非法获取 NovelPoster 的电子邮件和其他电子帐户。

原告在投诉书中所指控的行为违反联邦计算机欺诈和滥用法案，联邦电子通讯隐私法案，加利福尼亚州的第一至第四个行为原因全面的计算机数据访问和欺诈行为以及加利福尼亚州的入侵隐私法案。被告称 NovelPoster 未能根据“计算

机欺诈和滥用法案”和加利福尼亚州“940 全面计算机数据访问和欺诈法案”充分赔偿损失以支持其诉讼原因，并未恳求被告根据“电子通信隐私法”“截获”任何电子通信，加利福尼亚州的入侵隐私法案。

二、外文二次资源（Secondary Sources）

检索路径：westlaw——secondary sources——关键词"computer system" or "information system" or cybercrime 5/ destroy，共 98 个结果，经筛选：

- **期刊**

选用数据库：westlaw- secondary sources

关键词：“computer system”“information system”“destroy”

检索路径：westlaw——secondary sources——关键词"computer system" or "information system" or cybercrime 5/ destroy，

（1）Computers & Security Vol.20, No.8, pp.715-723, 2001

《Computer crimes theorizing》

A majority of computer crimes occur because a cur- rent employee of an organization has subverted exist- ing controls. By considering two case studies, this paper analyzes computer crimes resulting because of violations of safeguards by employees.The paper sug- gests that various technical, procedural and normative controls should be put in place to prevent illegal and malicious acts from taking place. Ultimately a good balance between various kinds of controls would help in instituting a cost-effective means to make both accidental and intentional misconduct difficult. This would also

ensure, wherever possible, individual accountability for all potentially sensitive negative actions.

大多数计算机犯罪的发生是因为组织的员工颠覆了现有的控制。该文通过对两个案例进行研究，文章分析了由于员工违反防范措施而导致的计算机犯罪。该文建议应采取各种技术、正式和非正式防范措施，防止非法和恶意行为的发生。最终，各种防范措施之间的良好平衡将有助于制定一种具有成本效益的手段，使意外和故意的不当行为难以实现。这也将确保在可能的情况下对所有潜在的负面行为进行个人责任追究。

（2） Computers Law & Security Review Vol 28,pp.201-208,2012

《Data attack of the cybercriminal: Investigating the digital currency of cybercrime》

First introduced the concept of the Cybercrime Execution Stack by examining in detail the underlying data objectives of the cybercriminal. Both technical and non-technical law enforcement investigators need the ability to contextualise and structure the illicit activities of the cybercriminal, in order to communicate this understanding amongst the wider law enforcement community. By identifying the potential value of electronic data to the cybercriminal, and discussing this data in the context of data collection, data supply and distribution, and data use, demonstrates the relevance and advantages of utilising an objective data perspective when investigating cybercrime.

本文的目的是通过对网络犯罪基本数据目标的详细考察，引入网络犯罪执行堆叠的概念。技术和非技术的执法调查人员都需要有能力将网络罪犯的非法活动

纳入背景并组织起来，以便在更广泛的执法领域之间传达这种理解。通过识别电子数据对网络犯罪的潜在价值，并在数据收集、数据供应和分发以及数据使用的背景下讨论这些数据，展示了在调查网络犯罪时利用客观数据视角的相关性和优势。

- **英文著作**

选用数据库：westlaw- secondary sources

关键词：“computer system”“information system”“destroy”

检索路径：westlaw——secondary sources——关键词"computer system" or "information system" or cybercrime 5/ destroy，

（1）《Cybercrime 》 Grabosky, Peter N.,

As computer-related crime becomes more important globally, both scholarly and journalistic accounts tend to focus on the ways in which the crime has been committed and how it could have been prevented. Very little has been written about what follows: the capture, possible extradition, prosecution, sentencing and incarceration of the cyber criminal. Originally published in 2004, this book provides an international study of the manner in which cyber criminals are dealt with by the judicial process. It is a sequel to the groundbreaking Electronic Theft: Unlawful Acquisition in Cyberspace by Grabosky, Smith and Dempsey (Cambridge University Press, 2001). Some of the most prominent cases from around the world are presented in an attempt to discern trends in the handling of cases, and common factors and problems that emerge during the processes of prosecution, trial and sentencing.

随着与计算机有关的犯罪在全球范围变得更加重要，学术和新闻报道都倾向于关注犯罪的实施方式以及如何防止犯罪。 关于以下内容几乎没有被写入：捕获，引渡，起诉，判刑和监禁网络罪犯。 该书主要提供了一个关于司法程序处理网络罪犯的方式的国际研究，提出来自世界各地的一些最突出的案件是为了辨别处理案件的趋势，以及在起诉，审判和判决过程中出现的共同因素和问题。

（2）《Principles of cybercrime》 Clough, Jonathan.

"Digital technology has transformed the way in which we socialise and do business. Proving the maxim that crime follows opportunity, virtually every advance has been accompanied by a corresponding niche to be exploited for criminal purposes; so-called 'cybercrimes'. Whether it be fraud, child pornography, stalking, criminal copyright infringement or attacks on computers themselves, criminals will find ways to exploit new technology. The challenge for all countries is to ensure their criminal laws keep pace. The challenge is a global one, and much can be learned from the experience of other jurisdictions. Focusing on Australia, Canada, the UK and the USA, this book provides a comprehensive analysis of the legal principles that apply to the prosecution of cybercrimes. This new edition has been fully revised to take into account changes in online offending, as well as new case law and legislation in this rapidly developing area of the law"--Provided by publisher.

数字技术已经改变了我们社交和做生意的方式，证明罪行符合机遇的准则，实际上每一次进步都伴随着一个相应的利基被用于犯罪目的;所谓的'网络犯罪'。如欺诈，儿童色情，跟踪，侵犯版权或侵犯计算机本身，罪犯将会找到开发新技术的方法，所有国家面临的挑战是确保他们的刑事法律保持同步，挑战是全球性

的，从其他司法管辖区的经验中学习，本书以澳大利亚，加拿大，英国和美国为重点，全面分析了适用于网络犯罪起诉的法律原则，并对此新版进行了充分修订，以考虑到网络犯罪的变化，以及这个快速发展的法律领域的新案例法和立法。

第五部分 总结

（一）关于破坏计算机信息系统罪，我国国内文献相对成熟，一次资源和二次资源比较丰富，可参考性强。关于该罪的界限尚没有清晰的规定。

（二）国外文献相对繁杂，虽然有计算机相关的保护法律，但没有控制计算机信息系统罪的相关罪名，需要利用相关关键词，仔细筛选。但国外有关计算机犯罪的法律相对成熟，可以在界定该罪上有所借鉴。

（三）国外的司法判例虽然有一定借鉴性，但仍有其特殊性，需要弄清其中原理，再进行参考。