摘　要

流量劫持是数字化社会发展过程中产生的新型犯罪现象，其中域名解析型流量劫持是实践较为常见的一种流量劫持行为类型，主要表现为DNS劫持，也被称为域名劫持，即侵入者通过劫持DNS服务器，获得对于某域名的解析控制，通过修改此域名的解析结果，使用户在对网络域名进行访问时浏览到错误的网页，造成网络运营商流量流失的危害结果，同时可能伴随用户个人的合法权益受到侵害。对此，传统的民商事法律行为无法实现法律目的的社会效果，因此只能尝试从刑法层面进行规制。

最高人民法院发布的102号指导案例为司法实务中的流量劫持，主要是DNS型流量劫持问题定性提供了基调，但由于受技术层面认知的约束，如对流量劫持的技术原理、类型特点以及本质的理解不足，导致部分案件在对DNS劫持的适用罪名上出现了争议和判决结果的偏颇。分歧主要集中在对破坏计算机信息系统罪和非法控制计算机信息罪的准确适用上。同一个劫持行为很有可能导致不同的犯罪结果的发生，因此想要判断流量劫持行为究竟最终应以何种罪名定罪则比较困难。这主要由于立法条文的简单化概述性规定与实践理解的差异性造成的混乱。对规范进行对比并结合实践案件分析，可明确辨明上述二罪法律条文中的行为对象、行为构成要素以及行为类型，所以二者实际存在本质区别。“非法控制”是行为人通过非法方式进入计算机信息系统内部进行排他性控制并使用，侵害系统机密性和可控性的行为；“破坏”是借助信息技术通过法定的三种行为类型，影响计算机信息系统的正常运行，侵害其完整性和可用性的行为。经上述区别便可有效解决对DNS型流量劫持的行为定性及刑罚适用问题，但在部分特殊情况下仍存在想象竞合的情况需予以特殊处理。

尽管实践中多数判例认为应适用破坏计算机信息系统罪，但却忽略了对行为人犯罪目的的评价。事实上行为人的犯罪目的不在于破坏计算即信息系统的安全或破坏网络管理秩序，而在于将劫取的网站流量进行出售以牟利，出售所劫流量与流量劫持二者是目的行为与手段行为的关系，因此有学者认为流量劫持应为侵犯财产犯罪，可对行为人以盗窃罪、破坏生产经营罪和诈骗罪定罪处罚。其中，盗窃罪需面对网站流量可以被评价为财产犯罪的保护对象这一难题，而破坏生产经营罪则需完善在互联网层面“其他方法”的破坏行为的类型解释，诈骗罪的适用又主要针对行为人通过流量劫持破坏计算机信息系统进而实施诈骗的情形。综上，流量劫持适用盗窃罪具备理论可行性但缺乏实践依据，而流量劫持的结果因无法实际支配生产经营无法构成破坏生产经营罪，而通过流量劫持实施诈骗因符

合手段行为与目的行为的逻辑，故构成牵连犯的情形在理论和实践均有据可循。

综合考虑流量劫持行为侵害的刑法保护法益、犯罪目的、行为本质、以刑法现实的计算机犯罪进行规制的优缺性，并结合司法实践具体案件的事实认定情况，流量劫持行为应形成以计算机类犯罪规制思路为主，财产犯罪规制思路为辅的类型化定罪模式。而在具体的罪数形态处理问题上，当破坏计算机信息系统罪涉及计算机犯罪的其他罪名的吸收或者想象竞合时，要按照相应的处断原则定罪量刑；当计算机犯罪与盗窃罪等财产类犯罪竞合以及通过计算机犯罪实施其他财产犯罪时，司法机关要把握好这两个基本点，分别按照想象竞合犯以及牵连犯的处断原则进行处理。

关键词：流量劫持，DNS，计算机信息系统，非法控制，破坏，财产性利益

Abstract

Traffic hijacking is a new criminal phenomenon in the process of the development of digital society." Domain Name Resolution "traffic hijacking is a type of the common traffic hijacking behaviors, mainly manifested as DNS hijacking, also known as domain name hijacking, which refers to hackers use some skills to hijack the DNS server to obtain the resolution control of domain names, then modify the resolution results of the domain name. When users visit the network domain name, they browse the wrong web page, resulting in the loss of network operators' traffic and the threatens of users' personal legitimate rights and interests. In this regard, traditional civil and commercial legal behaviors cannot achieve the social effect of legal purposes. Therefore we need to try to regulate from the level of criminal law.

The Guiding Case No. 102 issued by the Supreme People's Court has provided the keynote for the qualitative determination of DNS traffic hijacking in judicial practice. However, due to the constraints of technical cognition, such as the lack of understanding of the technical principle, type characteristics and essence of traffic hijacking, some cases have disputes and biased judgment results on applicable charges. The main disagreement centered on the precise application of the crime of damaging computer information system and the crime of illegally controlling computer information. The same hijacking behavior is likely to lead to different criminal results, so it is difficult to determine what charges should be used for DNS hijacking behavior. This is mainly due to the confusion caused by the difference between the simplified and summarized provisions of legislative provisions and the practical understanding. By comparing the norms and combining with the analysis of practical cases, we can clearly identify the object of behavior, the elements of behavior and the types of behavior in the legal provisions of the above two crimes, so there are essential differences between the two in fact. "Illegal control" refers to the behavior that the actor enters the computer information system by illegal means to control and use it exclusively, infringing the confidentiality and controllability of the system. "Sabotage" refers to the behavior that damages the normal operation, integrity and availability of computer information system by means of technology through legal behavior types. The above differences can effectively solve the qualitative behavior of DNS traffic hijacking and the application of penalty problems, but in some special cases there are still imaginary conjunctions which need special treatment.

Although most cases in practice hold that the crime of damaging computer information system should be applied, they ignore the evaluation of the criminal purpose of the perpetrator. In fact, the criminal purpose of the perpetrator is not to destroy the security of the computing or information system or disrupt the order of network management, but to sell the hijacked website traffic for profit. Selling the hijacked traffic and DNS hijacking are the relationship between the acts of purpose and means. Therefore, some scholars believe that DNS hijacking should be a crime of

property infringement. The perpetrator may be convicted and punished with the crimes of theft, sabotage of production and business operation and fraud. Among them, the crime of theft needs to face the problem that the website traffic can be evaluated as the object of protection of property crime, while the crime of damaging production and business needs to improve the type interpretation of the destructive behavior of "other methods" at the level of the Internet. The application of the crime of fraud is mainly aimed at the situation where the perpetrator destroys the computer information system through hijacking and then commits fraud. To sum up, the application of traffic hijacking to theft has theoretical feasibility but lacks practical basis, and the result of DNS hijacking cannot constitute the crime of damaging production and operation because it cannot actually control the production and operation, while the case that the fraud through DNS hijacking constitutes the crime of implicated crime because it conforms to the logic of means act and purpose act has evidence to follow in both theory and practice.

Considering the infringement of the interests of criminal law protection law, the purpose of crime, the nature of behavior of DNS traffic hijacking, the advantages and disadvantages of regulating computer crimes in the reality of criminal law, and combining with the fact determination of specific cases in judicial practice, traffic hijacking should form a type conviction model with the regulation thinking of computer crimes as the main, and the regulation thinking of property crimes as the secondary. When the crime of destroying computer information system involves the absorption or imaginary conjoint of other charges of computer crime, it should be convicted and sentenced according to the corresponding punishment principle. When the computer crime concurrence with theft and other property crimes and other property crimes are carried out through the computer crime, the judicial organs should grasp these two basic points and deal with them according to the principle of punishment of imaginary concurrence and implicated crime respectively.

Keywords: traffic hijacking, DNS， computer information system, illegal control, destruction, property interest

目录

引　言

一、　选题背景及目的

流量劫持是数字化社会发展过程中产生的法律问题，通常表现为行为人运用恶意软件或者程序修改用户浏览器、锁定主页或不停弹出新窗口等方式，强制用户访问某些网站，劫持并转移特定网络运营商经营网站的流量，将其出售给相关组织或个人牟取高昂的收入。域名解析型流量劫持是实践中较为常见的一种流量劫持的行为类型，主要表现为 DNS 劫持，即侵入者通过非法途径劫持 DNS 服务器，获得对于某网页、网站域名的解析记录控制权，进而修改该域名的解析地址，导致用户在对某网络域名或 IP 地址进行访问时就会进入到修改控制后的地址，最终访问错误的网页。

因流量劫持社会危害性的增强，传统的民商事处理手段已无法满足对法益保护的需求，因此需要从刑法层面对其进行规制。虽然最高人民法院 102 号指导案例的出台奠定了司法实务对于域名解析流量劫持定性的基调，但由于法院对流量劫持的技术原理、类型特点以及本质的理解不足，导致部分案件在罪名适用问题上出现了争议和偏差。在实践中，法院定性的主要分歧集中在破坏计算机信息系统罪和非法控制计算机信息罪。本文意在分析域名解析行为中流量劫持行为的本质及产生根源，并探寻破坏计算机信息系统罪与非法控制计算机信息系统罪二者的界限，特别是关于“破坏”与“非法控制”两种行为方式间的区分，做到对流量劫持行为的准确定性。同时评析理论界关于流量劫持行为以破坏生产经营罪以及财产犯罪入刑的观点，论证其可能性及优缺点，为流量劫持案件的定性问题提供思路与解决路径。

二、　研究现状

目前针对流量劫持的研究成果主要集中在国内。

在司法实践中，法院以往通常将“流量劫持”作为不正当竞争案件进行处理，该定性思路间接反映出此类行为发生的导火索。然而随着计算机信息技术的更新迭代以及互联网经济的迅猛发展，网站流量所呈现的商业价值与日俱增，仅将“流量劫持”理解为互联网企业为了争夺流量或关注度而进行的商业竞争行为，并单纯以民事手段予以规制已经无法满足实践以及网络经济发展的需求。因此，“流量劫持”行为入刑迫在眉睫。自 2015 年上海市浦东新区人民法院宣判了国内首例“流量劫持”刑事案件以来，实践中陆续出现类似 DNS 劫持案件，虽然数量不

多，但裁判机关对 DNS 劫持的行为定性和罪名适用等具体问题上存在分歧和争议，理论界对该现象亦予以关注和探讨。

从国内理论研究现状来看，因网络犯罪和计算机犯罪与传统犯罪相比专业性较强，故研究学者有限，而流量劫持的相关问题亦涉及部门法的衔接以及计算机专业技术理解，因此理论研究难度较大，学者们对于流量劫持行为的探讨也不广泛，因此在计算机犯罪领域，流量劫持是一个比较新兴的话题，其理论研究尚处于起步阶段，存在很大的发展空间。综合理论界的探讨，学者们对于流量劫持行为定性的探讨主要集中在民法和刑法两个部门法领域。

在全国首例流量劫持入刑案件的审理过程中就有观点认为流量劫持行为不构成犯罪。流量劫持行为人构成民事上的侵权行为或不正当竞争行为，仅应承担相应的民事责任，如民事赔偿、停止侵害。许多学者亦从流量劫持行为发生的实质出发，认为流量劫持应被定性为民商事活动中的不正当竞争。如王治国学者认为，“流量劫持作为新型网络不正当竞争手段，用于抢夺对手的市场份额，是流氓行径与强盗行为，是典型的不正当竞争。”[1]王斌学者认为“流量劫持并非简单地通过技术手段让用户访问 A 网站时跳转至 B 网站，在广义范畴里流量劫持是中国互联网发展过程中普遍存在的垄断、限制竞争方式。因此，一些互联网企业联名举报流量劫持的前提是他们自身应先遵守《反不正当竞争法》。”[2]以上代表学者的观点从流量劫持发生的原因入手进行了分析，因流量是互联网经营者竞争的着力点和目标，故流量劫持行为发生的根本目的在于行为人意图通过技术手段劫持或盗取本应属于与己方或第三方具有竞争关系或利益冲突网站的用户流量，使该部分流量被迫流向己方或第三方，从而为其增加收益，因此超出了正当的商业竞争的限度，打破了公平竞争的市场秩序，构成不正当竞争。

刑法理论界中，孙道萃学者认为，流量劫持一般是指劫持者利用各种木马插件、恶意程序不断弹出新窗口、修改浏览器设置、锁定网站主页，从而造成劫持网站流量损失的情形。并非所有的流量劫持行为均应当入罪，流量劫持在实施方法或实现技术上可以分为软性与硬性两种，软性的流量劫持并没有通过技术手段破坏用户的网络设备，而是采取核心关键词的替换等手段，这种流量劫持应当认定为不正当竞争。[3]当行为人采用 DNS 劫持、用户端植入插件或代码等手段时，这属于硬性的流量劫持，对计算机信息系统可能造成损害，涉嫌构成计算机类犯罪，如破坏计算机信息系统罪。此外提供流量劫持技术或帮助实施流量劫持的行为也可能构成犯罪。流量劫持作为典型的网络流氓行为，通过网络技术手段保持非法垄断地位或者非法侵占其他竞争对手的网络资源来牟取暴利，还可能构成破坏生产经营罪。叶良芳学者的观点与孙道萃学者有相似之处，其认为也应当对流

[1] 王治国：《浏览器主页被篡改锁定终于有人管了》，载《人民法院报》2015 年 11 月 11 日。
[2] 王斌：《流量劫持是中国互联网公司“特色”竞争方式》，载《通信世界》2016 年第 1 期，第 9 页。
[3] 参见孙道萃：《“流量劫持”的刑法规制和完善》，载《中国检察官》2016 年第 4 期，第 75 页。

量劫持根据技术手段的不同予以分类，对待不同种类的流量劫持应有不同定性。对于 DNS 劫持这种典型的域名解析流量劫持构成破坏计算机信息系统罪，而对于链路劫持则应当认定为不正当竞争。[4]大多数刑法学者们认为对于 DNS 流量劫持行为具有明确且较为严重的社会危害性：一方面可能侵犯网络用户的相关个人隐私以及财产利益，另一方面伴随流量的商业价值不断凸显，数据流量日益成为众多信息网站及服务网站争夺资源的背景下，其亦可能造成互联网运营商巨额的经济损失以及严重的名誉损毁。此外，劫持流量亦会引发对计算机信息系统造成规模性地控制或破坏、对网络市场秩序造成严重践踏的安全危机。故应当通过刑法对流量劫持行为予以规制，且选择计算机犯罪规制路径较为合理。

刘艳红学者认为流量劫持行为并没有破坏计算机信息系统的内在规则和正常使用，行为人只是短时间内利用各种恶意软件修改浏览器、锁定主页或不停弹出新窗口，以便劫取流量。该行为侵犯的主要是财产性利益，不符合破坏计算机信息系统罪的客观行为要件，应由相应的财产犯罪进行规制。[5]

于志刚学者认为流量劫持指的是“黑客通过网络链接技术使网络用户被迫或无意识地访问特定网站或网页，以此获得流量收入等利益。对于此种行为的评价，传统上首先从受到实体直接影响的网站、网民一侧进行思索。以网站为被害人的侧面观察，涉嫌构成破坏生产经营罪，以网民为被害人的侧面观察，可能构成诈骗罪。”[6]评价“流量劫持”的刑法性质，还需要变换视角来进行思索。拦截他人访问目标网站或者网页的行为，性质上属于在网络空间中实施寻衅滋事罪中的“拦截”他人的行为。

综上所述，刑法学者对流量劫持行为中流量的概念、劫持行为的表现方式争议不大，主要是对劫持行为的定性认识不一。大多学者认为，流量劫持行为是否构成犯罪要结合行为的手段、性质来判定，并非所有的流量劫持行为均需要用刑法手段来规制，对于危害性不大的劫持行为可认定为不正当竞争，危害性严重的可构成犯罪，可能构成破坏计算机信息系统罪、盗窃罪、破坏生产经营罪、寻衅滋事罪等罪。

三、 研究方法

本文主要立足于我国当前在规制流量劫持行为中所遇到的法律适用问题，综合运用多种分析研究方法，对流量劫持行为的概念、行为方式、惩罚规制等方面内容进行系统分析，为今后司法实践中处理相关案件提供参考意见。

第一，文献研究法。查找、收集、整理与流量劫持行为刑法定性问题相关的

[4] 参见叶良芳：《刑法教义学视角下流量劫持行为的性质研究》，载《中州学刊》2016 年第 8 期，第 46 页。

[5] 参见刘艳红：《网络时代刑法客观解释新塑造：“主观的客观解释论”》，载《法律科学》2017 年第 3 期，第 97 页。

[6] 于志刚、郭旨龙：《网络刑法的逻辑与经验》，中国法制出版社 2015 年版，第 236-241 页。

文献资料，梳理学者们的不同观点，分析学者们各自的论证角度，更全面地了解计算机犯罪相关理论知识，并进行思考，整理自己的研究思路。

第二，案例研究法。检索、收集和归纳涉及流量劫持行为的裁判文书，逐一分析，并对相关裁判文书进行整理分类，总结出司法实践中关于流量劫持行为定性问题存在的不同观点以及辩审冲突的焦点，选取典型案例进行细致分析。

第三，归纳分析法。通过对文献和裁判文书进行检视性阅读，归纳目前学界和司法实践中对于流量劫持行为定性问题的争议焦点，对不同观点进行整理。

四、 论文结构安排

第一部分在界定流量劫持，明确其概念与类型的基础上，提出域名解析行为中流量劫持行为刑法规制的现实问题。我国司法实践中对于流量劫持行为的处理，以往主要通过民事措施来解决。2015 年上海市浦东新区法院判决的我国流量劫持入刑第一案，可以说具有里程碑式的意义，成为惩处此类案件的司法标杆。然而对此案也有不少质疑。目前司法实践和理论界对流量劫持行为的争议焦点有二：一是流量劫持行为是否构成犯罪；二是在构成犯罪的前提下，究竟构成何种具体犯罪？刑法应采取怎样的规制路径？

第二部分在于分析并解答第一部分提出的两个争议点。在分析第一个争议点时首先对实务界和理论界关于流量劫持罪与非罪观点进行整理和评析；其次通过阐述域名解析流量劫持侵害的法益和民事诉讼对规制该行为的局限性两方面，来说明本文认为以刑法规制 DNS 流量劫持行为的必要性。在分析第二个争议点时思路有所不同，关于 DNS 型流量劫持究竟适用何种罪名的问题上，实务界和理论界观点有所出入。司法实践偏向于用计算机犯罪进行规制，在具体适用破坏计算机信息系统罪还是非法控制计算机信息系统罪产生分歧，并结合典型案例进行审视；理论界大多数学者也赞同用计算机犯罪进行规制，除此观点外，还有学者认为可以通过财产犯罪进行规制，在此对代表性观点予以评析。在第二部分结尾，通过分析以上两个争议点，可以总结出 DNS 流量劫持在实践中出现司法困局以及理论界出现分歧的原因，主要有以下三点：一是劫持手段本身比较复杂，实践中存在两个罪名发生想象竞合的情形，加之已有的两种定罪思路存在论证瑕疵，因此实践中对于流量劫持的定性有不同的意见；二是非法控制计算机信息系统罪与破坏计算机信息系统罪在立法规定上较为粗疏，忽视了对相关概念的界定与解读，暴露了网络刑法规范的针对性和专业性不足；三是理论界之所以会对流量劫持有不同的定性思路，关键在于对流量劫持侵害的法益有不同的认识，因为流量劫持侵害的法益是多重的。

第三部分进一步围绕前述第二个焦点问题，重点探讨 DNS 流量劫持行为的刑法规制路径，总结发现对于流量劫持行为主要有以计算机类犯罪论处与以财产犯

罪论处两类不同的定性思路。对于计算机类犯罪规制思路，首先分析了其保护的法益与流量劫持侵害的法益存在对应；其次对破坏计算机信息系统罪与非法控制计算机信息系统罪的构成要件进行阐述，提出本文关于两罪相关的关键概念的理解，特别对“破坏行为”和“非法控制行为”进行了重点分析和区分，并结合实践案例明晰二者所规制的具体情形；最后针对“破坏”与“非法控制”竞合的原因进行讨论，在通过对二者关系进行梳理过程中发现，虽然在行为本质、行为构造和模式上均有不同，但内在存在联系，二者是辩证的关系而非截然对立的关系，实践中存在想象竞合的情况，应根据想象竞合的处理原则进行定罪。对于适用财产类犯罪规制思路的可能性，通过分析认为流量劫持单纯被定性为财产类犯罪困难较大，特别是盗窃罪不仅存在理论争议还存在实践操作难题，而破坏生产经营罪的适用可能性也比较小，但存在利用非法控制或破坏计算机信息系统去实施诈骗进而构成牵连犯的可能性。

第四部分即观点总结部分，本文认为在处理实践中的 DNS 劫持案件时，应遵循“一体三面”的思路，即以破坏计算机信息系统罪为重点规制罪名，在特殊情形下需要考虑罪数问题。当破坏计算机信息系统罪与其他计算机类犯罪发生竞合时，应按照相应的处断原则定罪处罚。而当破坏计算机信息系统罪与其他财产犯罪发生想象竞合时，按照通说的一般处断原则应从一重处。当行为人通过流量劫持破坏计算机信息系统的手段实施财产犯罪时，二者是牵连犯的构造，按照从一重处重罚的原则进行定罪量刑。

一、 问题的提出

流量劫持并非是一个法定概念，其仅仅是网络领域内的一种技术手段。流量劫持这一现象最早出现在法律领域是因2013年发生的百度诉奇虎不正当竞争一案，在该案的审理过程中，法院将奇虎公司在网址导航站的百度搜索框内设置直接指向奇虎公司网页内容的下拉提示词等行为认定为了流量劫持。很显然，这里被劫持的流量是网站流量，即互联网用户对百度的访问量。在互联网技术高速发展的今天，一个网站的流量是决定改网站价值的决定性因素，它承载的不仅仅是单纯的数据，更多的是互联网公司的商业价值以及互联网平台的利益。对于互联网企业来说，流量的财产价值已经在投资市场上获得了认可，显然已经成为决定企业被投资价值的重要因素，[7]因此成为企业间竞相争夺的商业资源，遂最终直接导致近年来围绕流量产生的民事纠纷和刑事纠纷案件的增加。

（一） 全国首例流量劫持行为入刑案引发的争议

案例一：付某、黄某破坏计算机信息系统案[8]

由于目前在互联网层面流量劫持行为愈加频繁多发、层出不穷，流量劫持的种类也是复杂多样，且不同种类的流量劫持因其所利用和依赖的技术手段的牵连在范围上有所交叉和重叠。为应对司法实践中对常见的流量劫持定性行为的难题，理论界依据各自的区分标准对流量劫持行为了一定的分类。有的学者根据劫持手段的性质将流量劫持划分为软性劫持和硬性劫持；[9]根据流量劫持的实施主体将流量劫持划分为网络服务提供商劫持和第三方劫持；[10]有的学者以流量劫持所利用的技术手段为标准，将其划分为DNS劫持、CDN劫持和网关劫持等。[11]而该案是典型的流量劫持中的DNS流量劫持情形，DNS流量劫持也是司法实践中最

---

[7] 参见季境：《互联网新型财产利益形态的法律建构——以流量确权规则的提出为视角》，载《法律科学（西北政法大学学报）》2016年第3期，第183页。

[8] 案情简介：在此案中被告人付某、黄某等人租赁数个服务器，通过相关的技术手段，使用恶意代码更改互联网用户路由器的DNS系统装置，导致用户在登录“2345.com”等导航网站时被强行跳至其设定的“5w.com”导航网站，被告人随后将所获的互联网用户流量与杭州某科技有限公司（“5w.com”导航网站所有者）进行交易，其非法收入共计754762.34元。

[9] 参见孙道萃：《“流量劫持”的刑法规制和完善》，载《中国检察官》2016年第4期，第75页。

[10] 参见叶良芳：《刑法教义学视角下流量劫持行为的性质研究》，载《中州学刊》2016年第8期，第46页。

[11] 参见陈禹衡：《流量劫持的刑法规制思考——以第102号指导性案例为视角》，载《西南石油大学学报（社会科学版）》2019年第6期，第78—79页。

为常见和多发的流量劫持类型。该案件中行为人的劫持过程可通过下图予以简单演示。

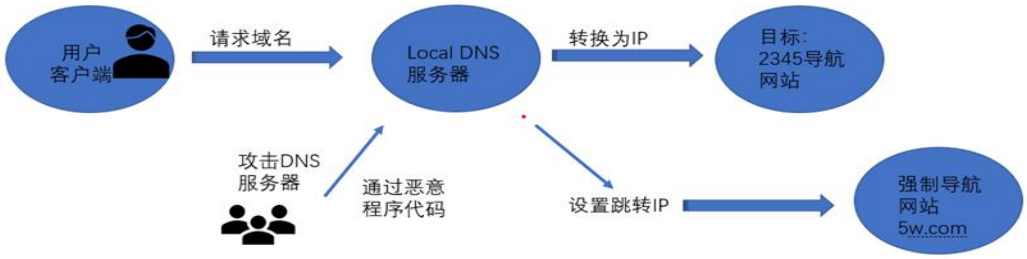

图 1 案例一中被告人行为分析演示图

裁判机关于 2015 年做出判决，认为两名被告使用恶意代码修改互联网用户路由器的 DNS 设置，将用户访问“2345.com”等导航网站的流量劫持到所设置的“5w.com”导航网站的行为明显影响并破坏了用户的计算机信息系统功能（DNS 系统解析功能），导致计算机信息系统不能按照原有的设置程序正常工作，DNS 系统无法正常解析文件，符合破坏计算机信息系统罪的客观行为要求。[12]该案件是当时我国第一起流量劫持适用刑法规制的案件，是计算机犯罪领域具有里程碑意义的判决，因其影响力重大，被最高人民法院确立为第 102 号指导案例。

该案一经宣判，便引起了实务部门和理论界的热议。然而，司法实践引发的争议不是负面的，通过分析法院针对类似案件的不同分析思路和判决有利于我们深层次了解流量劫持，厘清现阶段裁判出现的问题，这对于推动司法进步具有重大意义。通过梳理可以发现，该案引发的司法实践和理论界关于流量劫持行为的定性意见主要表现在以下两个争议焦点：

第一，是否应对流量劫持行为予以刑法规制。在上述案例一宣判之前，流量劫持从未踏足过刑法规制领域的边界，司法实践通常适用民法或者反不正当竞争法对其进行规制。因此许多民法学者及经济法学者质疑通过刑法对流量劫持进行规制的合理性以及必要性，这是关于流量劫持的罪与非罪之争。

第二，在肯定流量劫持可以由刑法进行规制的前提下，对流量劫持应以何罪定性。巧合的是，在全国首例流量劫持入刑案件发生之后，几乎在同一时间也发生一起以 DNS 流量劫持手段实施的流量劫持案件，但是审判机关将案件定性为非法控制计算机信息系统罪。理论界还有观点认为流量劫持应适用财产犯罪才能更

[12] 参见付宣豪、黄子超破坏计算机信息系统案，最高人民法院指导案例 102 号（2018 年）。

好地保护法益，究竟采用何种罪名才能更好地规制流量劫持，这是关于流量劫持的罪名适用之争。

（二） 流量劫持行为司法实践定罪现状

百度诉 360 违反 Robots 协议案的宣判使得流量劫持这种技术首次受到法律的规制，但其意在规制的是企业间的不正当竞争行为，特别是实践中比较常见的“搭便车”现象，即通过对目标网页设置插标或在其搜索框下下拉关键词从而诱导网络用户本意浏览目标网页时却访问了其他网站，从而实现目标网站浏览量的分流。因这种诱导型的流量劫持主要发生在民商事领域的企业竞争中，主要影响到网民的信息选择自由权以及网上冲浪体验，因此司法实践认为其社会危害性相对较小，多采用民事手段进行规制。但 DNS 劫持手段的出现和运用使得司法机关逐渐意识到流量劫持严重的社会危害性进而采用刑事手段对其进行规制。根据上文中学者们的分类，诱导型属于软性劫持，而 DNS 劫持则属于硬性劫持，二者的技术性质和造成的危害结果有着明显不同，硬性劫持的社会危害性更为显著。借助“聚法”以及“威科先行”等案例检索平台，以“流量劫持”为关键词进行案例检索可以发现，截至 2022 年 8 月共查询到有效裁判文书 51 份，其中民事案件 39 份，刑事案件 12 份。将各案的判决时间线条进行梳理可以看到，2015 年之前司法机关对于流量劫持更多作为民事案由中的不正当竞争以及知识产权纠纷进行定性并裁判，而 2015 年之后，随着首例入刑案件的宣判，司法机关逐渐运用刑事手段对流量劫持进行规制。具体案件分布情况可参照图 2。

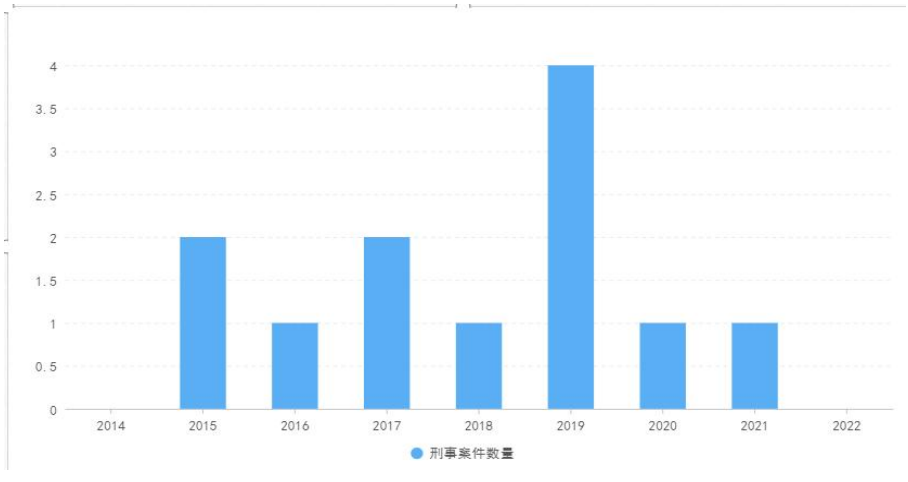

图 2 流量劫持刑事案件数量情况

而付某案的宣判不仅使得实务界和理论界对流量劫持的认知视角从民法领域转移到刑法领域，并且引发了学者们针对流量劫持行为定性问题更加深入的思考和学术探索，可谓具备重大的实践价值和理论价值，是计算机犯罪领域具有里程碑意义的判决，因其影响力重大于 2018 年被最高人民法院确立为第 102 号指导案例，从图 2 中可以看到受指导案例的影响，2019 年裁判的刑事流量劫持案件数量明显增多。

虽然最高人民法院的指导案例的发布具有重要的参考意义，但是从实践中司法机关针对流量劫持的定性结果来看，还是存在一定差异。在目前可检索查阅到的案例裁判文书中，出现了破坏计算机信息系统罪、非法控制计算机信息系统罪、非法获取计算机信息系统数据罪以及帮助信息网络活动罪等不同罪名定罪，具体的案件定罪结果分布情况可参照图 3。

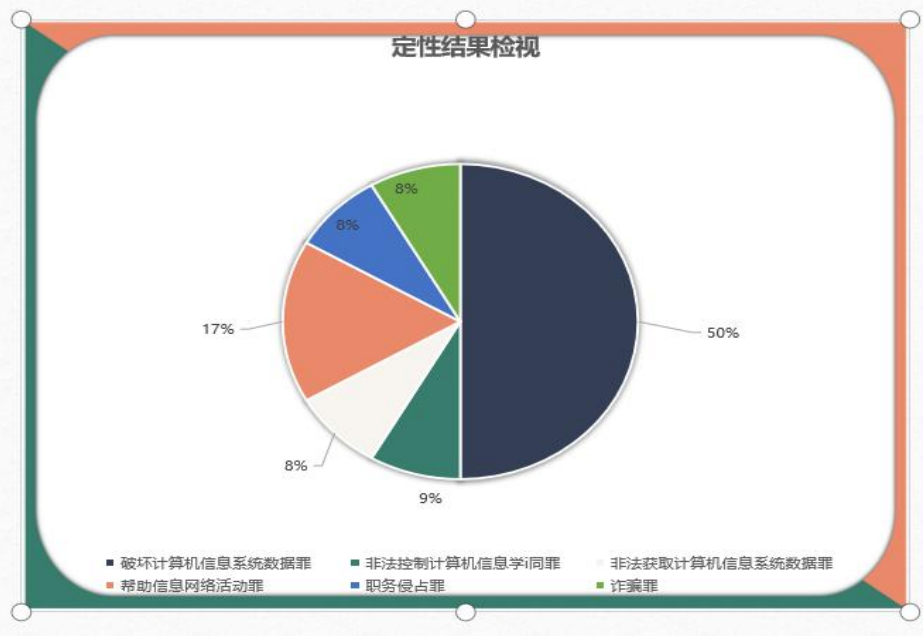

图 3 流量劫持刑事案件定性结果

特别是针对指导案例中被告人使用的 DNS 劫持技术手段的定性意见不同的法院产生了破坏计算机信息系统罪与非法控制计算机信息系统罪的分歧，问题是在各自的裁判文书中均缺少对流量劫持定罪意见的充分论证。面对司法实践存在的争议不应该无视或者回避，相反，通过分析法院针对类似案件的不同分析思路和判决有利于我们深层次了解流量劫持，厘清现阶段裁判出现的问题，这对于推动司法进步具有重大意义。

二、 流量劫持行为定罪之争

通过上文的论述可以明晰，关于流量劫持，实务界和理论界主要有两个探讨的争议焦点：其一是流量劫持的罪与非罪之争，即应该通过民事手段还是刑事手段进行规制；其二是刑法学者在主张刑事规制的前提下的罪名适用之争，目前出现了财产犯罪和计算机犯罪的不同规制观点，下文将着重对两个争议焦点进行论述和分析。

（一） 流量劫持行为罪与非罪之争

1. 罪与非罪观点聚讼

在付某案宣判之前，流量劫持从未踏足过刑法规制领域的边界，立法也主要将该类行为限定在不正当竞争领域，[13]司法实践通常适用民事手段对其继续规制。比如此前广受热议的百度诉 360 案，淘宝诉帮 5 买案，均通过相应的民事赔偿以及民事诉前禁止令等手段进行救济。许多民法学者从流量劫持行为发生的实质出发，认为流量劫持应被定性为民商事活动中的不正当竞争。[14]此类观点主要从流量劫持发生的原因入手进行了分析，因流量是互联网经营者竞争的着力点和目标，故流量劫持发生的根本目的在于通过技术手段劫持本应属于竞争对手的用户流量，使流量被迫流向特定对象，从而为其增加收益，因此超出了正当的商业竞争的限度，构成不正当竞争。并且从司法实践具体情况分析发现，流量劫持行为被判处不正当竞争的案件中具体的技术手段多表现为链路劫持，即一种引诱型劫持，因其通过插入连接或推送广告主要干扰到网民上网的信息自主选择权，为网名造成不好的冲浪体验，社会危害性较小，故从刑法谦抑性的角度出发，刑法不应过多干预民商事活动，对于流量劫持应当采取传统的民事规制手段。

大多数刑法学者考虑到如使用 DNS 劫持手段的部分流量劫持类型的社会危害性较大，表示出对此类流量劫持行为入刑的赞同和认可。孙道萃和叶良芳学者

---

[13] 《反不正当竞争法》第 12 条第 2 款第 1 项
经营者不得利用技术手段，通过影响用户选择或者其他方式实施未经其他经营者同意的，在其合法提供的网络产品或者服务中插入链接、强制进行目标跳转的行为。

[14] 参见王治国：《浏览器主页被篡改锁定终于有人管了》，载《人民法院报》2015 年 11 月 11 日；王斌：《流量劫持是中国互联网公司“特色”竞争方式》，载《通信世界》2016 年第 1 期，第 9 页。

更为细致地对流量劫持根据技术手段的不同而予以分类，主张对待不同种类的流量劫持应有不同定性。[15]对于 DNS 劫持这种典型的域名解析流量劫持构成破坏计算机信息系统罪，而对于危害性较小的软性流量劫持则应当认定为不正当竞争。本文虽探讨流量劫持行为的定罪问题，但通过引入最高法的指导性案例，在文章论证过程中结合诸多案例，重点分析司法实践涉及的流量劫持中较为典型和最为广泛的 DNS 劫持产生的争议和理论难题。理论界中，学者们大多使用流量劫持这一统一概念分析论证，未对具体概念做细致区分说明。针对流量劫持，大多数刑法学者们认为此行为具有明确且较为严重的社会危害性：一方面可能侵犯网络用户的相关个人隐私以及财产利益，另一方面伴随流量的商业价值不断凸显，数据流量日益成为众多信息网站及服务网站争夺资源的背景下，其亦可能造成互联网运营商巨额的经济损失以及严重的名誉损毁。此外，劫持流量亦会引发对计算机信息系统造成规模性地控制或破坏、对网络市场秩序造成严重践踏的安全危机，应当通过刑法予以规制。

事实上，通过此前对流量劫持的相关民事判决进行总结可以发现，被告人所承担的责任主要体现在因流量劫持对受害网站运营商造成了一系列的经济损失所承担的民事赔偿。由于刑法具有谦抑性，在司法实践中，承担民事法律责任是裁判机关综合研判流量劫持案件情节较轻、社会危害性较小时所采取的一种处理手段。但在当今互联网发展的形势下，网络犯罪越来越频繁，犯罪数额亦愈加膨胀，通过民法以及不正当竞争法对流量劫持进行规制，虽然有利于维护网络平台企业之间特别是互联网行业公平竞争的秩序以及相对自由发展的愿望，但是这对于互联网用户的合法权益（如个人隐私和相关财产利益）、网络企业的合法权益以及整个网络空间安全与秩序的保护力度却是无法满足的。而且通过民事赔偿的方法虽然可以在一定程度上挽救网络运营商的经济损失，但其制裁的主要是具备竞争关系的网络企业平台，而真正实施流量劫持的是黑客，是企业背后的“魔爪”，民事救济根本无法惩罚并威慑黑客，更加无法限制流量劫持的继续发生，无法起到相应的警示作用。因此，通过刑法规制流量劫持行为势在必行。

2. 侵害法益考察

[15] 参见叶良芳：《刑法教义学视角下流量劫持行为的性质研究》，载《中州学刊》2016 年第 8 期，第 46 页；孙道萃：《“流量劫持”的刑法规制和完善》，载《中国检察官》2016 年第 4 期，第 75 页。

刑法是为了保护相应的法益而设立的，[16]刑法分则中的每个条文均有各自所重视和保护的社会利益。要想对流量劫持行为准确定性，首先要分析其侵害的法益究竟是什么。目前学界对于流量劫持所侵害的法益主要有以下几种观点：

一是侵犯了用户的个人财产权益，持这种观点的学者主要考虑的是能否对流量劫持定性为盗窃罪等财产类犯罪的问题。而这里首先必须解决的是网络流量的性质。有的学者认为流量是一种财产性利益，其虽然不能完全等同于盗窃罪中的“财物”概念，但是作为网络运行商对用户提供的一种网络服务，其更像是一种财产性利益。[17]有的学者认为流量是一种网络虚拟财产，[18]还有的学者认为流量就是一种财物，即一种特殊的无体物，是具有价值和使用价值以及管理可能性的财物，与其他虚拟财产一样，不仅需要民法其进行保护，更需要刑法将其纳入管制范围。[19]虽然以上三种观点各有各的道理，但即便肯定流量的财产属性，单纯地将流量劫持定性为盗窃罪也存在不妥之处，因流量劫持的主要目的是让用户强制访问特定的网址进而增加该网站的访问量，虽然这一行为伴随着用户网络流量的流失，但却是微乎其微的，其数额也是难以统计的。故与其认为流量劫持侵犯了网络用户的财产权益倒不如认为侵犯了网络运营商的财产权益，论证网站流量的性质。上文论述到流量劫持“劫”的主要是网站流量，而用户的网络流量是附带的，网站流量是决定网站价值的决定性因素，网络运营商可以在相应的网站上投放广告，而网站广告的计费则由网络用户的点击量和访问量决定，而这些均能够相应地转化为网络运营商的收入，可以说网站流量与运营商的收入是紧密关联的。从司法实践来看，流量劫持行为劫持了网络运营商的网站流量，均造成了运营商巨大的经济损失，因此可以说流量劫持更多地是侵犯了网络运营商的财产利益，刘艳红学者也持此种观点[20]。

二是侵犯了计算机信息系统管理秩序或制度，持此观点的学者认为从最高人民法院第 102 号指导性案例的裁判结果分析，破坏计算机信息系统罪位于刑法分则第六章—妨害社会管理秩序罪，而互联网和现实社会一样同样存在某种程度上

[16] 参见张明楷：《行为无价值论与结果无价值论》，北京大学出版社 2021 年版，第 3 页。
[17] 参见赵文胜、梁根林、曲新久等：《盗窃“流量包”等虚拟财产如何适用法律》，载《人民检察》2014 年第 4 期，第 42 页。
[18] 参见张明楷：《非法获取虚拟财产的行为性质》，载《中国检察官》2015 年第 11 期，第 15-25 页。
[19] 参见谭宇：《刑法学视域下侵害网络流量问题研究》，载《太原理工大学学报（社会科学版）》2016 年第 3 期，第 21-23 页。
[20] 参见刘艳红：《网络时代刑法客观解释新塑造：“主观的客观解释论”》，载《法律科学》2017 年第 3 期，第 97 页。

的管理秩序，网络秩序甚至是公共秩序的重要组成部分。[21]用户和服务商在互联网社会均有着相应的权利和义务，并要严格遵守互联网规范。而流量劫持的使用则打破了互联网层面公平竞争、合法有序的规则，使用户和服务商的合法权益受到损害，造成网络秩序的不安和混乱。

三是侵犯了计算机信息系统的安全，目前这一观点占据主流地位。王作富学者认为，破坏计算机信息系统罪虽然被设置在妨害社会管理秩序罪章节中，但该罪实质是为了保护计算机信息系统的安全。[22] 随着互联网的迅猛发展和对社会生活的不断介入，目前许多基础设施均要依赖互联网的运转和工作，行为人一旦对网络服务器以及其他基础设施进行攻击，将会严重损害到计算机信息系统的安全，倘若系统崩溃瘫痪将会对网络服务商乃至整个互联网行业造成无法挽回的损失。

可以说，以上观点各有其合理之处，将单一法益作为规制流量劫持行为的前提无法满足司法实践对法益保护的需要。事实上流量劫持行为不仅会对计算机信息系统的安全造成威胁,还可能侵犯系统内数据的秘密性、可使用性和完整性，同时也使网站运营商受到巨大经济损失。流量劫持行为侵害的法益不是单一的，而是多元的，包括网站运营商的财产性利益、网络用户的合法权益、计算机信息系统安全以及互联网的管理秩序。因此为了维护网络安全，有必要将流量劫持行为纳入刑法调整的范围。

3. 入罪应当性分析

持入罪赞成说的学者们之所以主张将流量劫持行为应纳入到刑法规制范围，主要考虑到其具备现实规制紧迫性以及理论依据。

流量劫持作为一种信息技术主要发生在互联网领域，其实对于此类网络不正当行为都有前置的相关网络监管、网络安全保护、公民个人信息保护等行政法规予以规制。但就现实状况来看，前置法的规制效果并没有达到预期。在巨大的经济效益面前，民事赔偿无法遏制网络平台对于金钱的渴望与贪婪，流量劫持无法得到有效规制。即便是如链路劫持等软性流量劫持，其虽然相较于 DNS 劫持等硬性劫持不会迫使用户强制跳转到特定网页，而是采用插入相关广告链接、弹窗等

[21] 参见张向东：《利用信息网络实施寻衅滋事犯罪若干问题探析》，载《法律适用》2013 年第 11 期，第 13-14 页。
[22] 参见王作富：《刑法分则实务研究》，中国方正出版社 2006 年版，第 226 页。

手段引诱用户访问特定网页，不会造成相关系统功能的损毁，但在链路劫持实现过程中仍然无法避免系统内数据被修改的环节，因此用户同样面临网络安全的威胁，如相关信息的泄露。因此基于维护网络安全的需要，流量劫持入刑具有现实紧迫性。

此外，我国刑法立法对成立犯罪的标准采用的是社会危害性说，可以说没有社会危害性就没有犯罪，社会危害性没有达到相当的程度，也不构成犯罪。以最高人民法院第 102 号指导案例为例，行为人通过恶意软件或程序侵入用户计算机的域名解析系统，恶意篡改解析 IP 数据结果的行为，其社会危害性主要体现在以下三个方面：

对网络用户自身而言，其计算机信息系统内部的某些设置遭受了攻击和破坏，不仅影响到用户的上网体验，更加对用户的网络安全造成巨大威胁，直接造成对用户个人信息和财产的安全隐患。

对网络企业和相关运营商而言，不仅导致网站访问量的损失，干扰企业正常的经济效益，抢占企业的市场占有率，甚至用户会因不了解实情因上网体验的影响对企业造成负面的评价，损毁企业的商业形象和信誉， 给企业造成无法弥补的损失。

对网络管理秩序而言，侵入者违背了自己同样身为网络用户对网络冲浪规则的遵守，通过恶意程序代码、恶意插件和病毒攻击其他用户和网站计算机信息系统的相关设置，是对网络管理秩序的严重破坏和践踏，2010 年“百度域名被劫持”事件就是典型的例证，其造成了百度系统近 5 个小时的瘫痪，性质极其恶劣。

鉴于流量劫持侵害的是多元法益，具有严重的社会危害性，故有必要将其纳入刑法的规制范围。电子化和数据化社会的发展给人们生活方式带来便宜的同时，也带来了更高的风险，特别是犯罪手段逐渐呈现出现代化和科技化特征。就目前来看，传统的犯罪方法已经被高新技术犯罪所取代，黑客入侵篡改数据、窃取资金，投放病毒破坏程序等方式呈现出蔓延之势。此类犯罪不仅隐蔽性强、投入少、获利高，还极易引起人民的不安和恐慌，司法机关必须予以重视和规制，才能保护好人民群众和社会的财产安全，巩固和稳定好社会秩序。

（二）流量劫持行为罪名适用之争

在肯定流量劫持有必要纳入刑法的规制范围的前提下，对其又该以何种罪名定性，实务界和理论界有不同的意见。

1. 司法实践定罪分歧

实务界对于流量劫持具体定罪的争议主要体现在应该适用计算机犯罪中的何种罪名，可见，实务界更注重保护计算机信息系统的安全运行以及对相关管理制度的维护。针对实践中多发的 DNS 劫持手段，司法实践主要有以下两条定罪路径：

（1） 破坏计算机信息系统罪

此类意见和实践以最高人民法院第 102 号指导案例为代表，也即上文论述的案例一付某案，从案件的具体分析来看法院的这一结论并无不妥之处，法院的处理结果也并无不当之处，但仔细研读判决书原文可以发现两个比较明显的问题：

第一，缺乏定罪的充分论证。从判决书原文来看，法院在认定基本的案件事实和认可相关的证据之后，通过列明并简单论证了被告人利用的手段和行为外在特征便做出破坏计算机信息系统罪的裁判认定结果，而缺少从构成要件层面对罪名适用的详细解释和论证，理论论证深度不足。

第二，缺乏对“流量劫持”的进一步解释和说明。“流量劫持”仅仅是计算机技术层面的一个概念，无论是刑事相关立法还是刑法理论界均缺少对其内涵和本质的解读。简言之，流量劫持并非是一个法定概念，且大多数人对其相关技术原理和基本理论并不知晓。而作为全国首件将流量劫持入刑的案件，如果未对流量劫持的行为过程和刑法具体定性进行论证和说明，对今后其他案例的指导会有一定的影响，特别是如果没有明确的标准和参考在司法适用上容易出现认定混乱的现象。

正是由于以上判决书中存在的问题，引发了理论界和实务界诸多对于该案裁判结果的争议。

（2） 非法控制计算机信息系统罪

案例二：施某等非法控制计算机信息系统案[23]

该案中，行为人同样采取了 DNS 劫持的手段，通过编辑更改 DNS 系统的域名解析文件，导致用户在浏览网站时被强制跳转，而重庆市渝北区人民法院却认为施某的行为符合非法控制计算机信息系统罪的构成要件，并以此对被告人定罪。[24]为方便理解 DNS 劫持的手段方式和行为过程，可参考图 4。

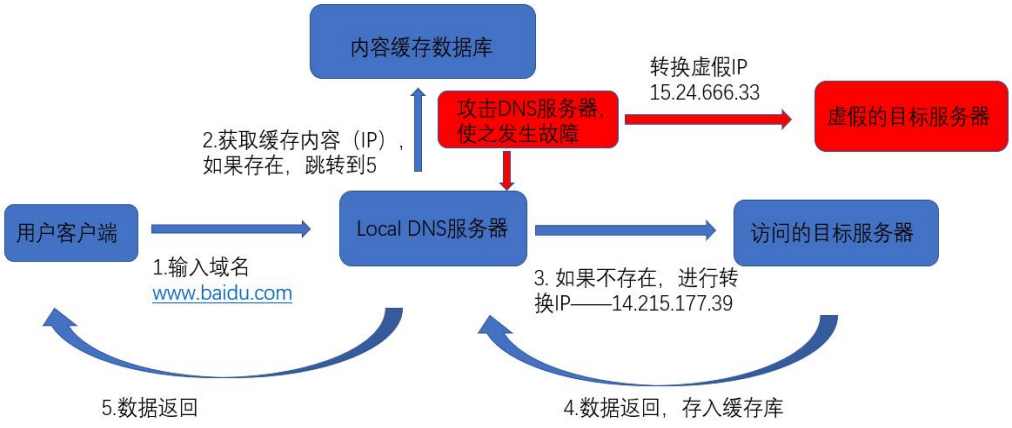

图 4 DNS 域名劫持过程

上述两个案件几乎发生在同一时间段内，通过比较可以发现其共性在于行为人均采用 DNS 劫持手段入侵用户计算机内的 DNS 系统，修改其中的相关数据，使系统原本应该正常解析域名的功能无法正常发挥。问题是，为什么一家法院会将 DNS 劫持认定为对计算机信息系统的“破坏”行为，而另一家法院认定为对计算机信息系统的“非法控制”行为？

从两起案件的裁判文书对比来看，法院虽然对流量劫持做了行为定性，但在裁判说理部分并不充分，既没有点明流量劫持行为的本质，也没有详细论证为何要适用该罪名。综合比较两起案件的全部内容，最大的区别在于，案例二中施某利用职务上的便利直接登录公司系统进行相关操作，而案例一中付某等人所采取的是使用恶意代码等技术手段从外部攻击入侵系统进而修改 DNS 服务器的相关

[23] 案情简介：被告人施某是某有限公司重庆网络监测维护中心核心平台部工作人员，负责业务平台数据配置。在其他被告人的引诱邀请下，施某利用职务的便利性，多次进入公司的 DNS 系统实施 DNS 域名的劫持，违规修改域名解析系统的配置文件，使得用户在访问相关网站时被强行跳至传奇游戏的私服网站，与其他被告人共获得了近 200 万的非法利益。

[24] 参见施硕等非法控制计算机信息系统案，重庆市渝北区人民法院刑事一审判决书，（2015）渝北法刑初字第 00666 号。

设置。总体来看施某所利用手段本身对计算机信息系统的破坏性较小，但这是否会实际影响实践中对于两罪的判断和适用？“非法控制”和“破坏”之间存在何种差异和联系？要想回答这个问题，必然涉及对两个罪名构成要件的规范解释。只有立足立法旨意，准确寻找两者规制的侧重点和异同，才能理性评价案件的行为定性。

2. 司法实践引发的理论争鸣

相比于实务界单纯地将定罪视角聚焦到计算机犯罪领域，理论界对流量劫持的定罪思路进行了充分的思考和研究，不仅涵盖上述实务界所探讨的关于破坏计算机信息系统罪与非法控制计算机信息系统罪的争议，还探索了对流量劫持适用财产犯罪规制路径的可能性，主要有以下几种代表性观点：

（1） 盗窃罪

持盗窃罪观点的学者主要从流量劫持发生的根源出发进行分析，流量劫持虽能够实现网页分流，但本意在于抢占流量，提升网络企业自身的竞争力。而网站流量对于网络企业自身来说承载了巨大的商业价值。比如刘艳红学者认为流量劫持行为并没有破坏计算机信息系统的内在规则和正常使用，行为人只是短时间内利用各种恶意软件修改浏览器、锁定主页或不停弹出新窗口，以便劫取流量。[25]该行为侵犯的主要是网络层面的财产性利益，不符合破坏计算机信息系统罪的客观行为要件和主观犯罪目的，应由相应的财产犯罪进行规制。然而这里又引申了一个新的理论问题值得思考，即网站流量的法律属性是什么，它是否是盗窃罪所保护的客体，这个问题将在后文进行详细探讨。

（2） 破坏生产经营罪

持破坏生产经营罪的学者代表主要是孙道萃学者和于志刚学者，其主要的论证思路在于流量劫持是一种典型的网络流氓行为，其本质是通过技术手段非法抢占自己在互联网行业的垄断地位或者恶意侵占竞争对手的资源。这样一种极其恶劣的不正当竞争行为如果任由其发展，必将严重破坏互联网正常的经营运行秩序，这不仅会损害互联网企业间公平发展、良好竞争的环境，还会对网络用户的合法权益造成威胁。因此即使行为人不采取类似于 DNS 劫持对计算机信息系统会造成破坏的技术手段实施流量劫持，也同样具有刑法规制可能性，可能涉嫌构成

[25] 参见刘艳红：《网络时代刑法客观解释新塑造：“主观的客观解释论”》，载《法律科学》2017 年第 3 期，第 97 页。

破坏生产经营罪。[26]可以说，此观点是孙学者对流量劫持定性的一种补充性思考，其重点还是强调了刑法对流量劫持规制的必要性，但观点本身对于流量劫持为何构成破坏生产经营罪没有进行细致的论证，因此后文会藉此探讨适用破坏生产经营罪的思路以及理论可行性论证。

（三） 流量劫持行为定罪分歧原因梳理

1. 流量劫持行为模式复杂多样

流量劫持本身就是一个比较复杂的技术手段，其行为方式多种多样，实践中也存在不同的类型，且不同类型的流量劫持在技术方式上又有交叉，实现效果上也有所出入，同一个劫持行为很有可能导致不同的犯罪结果的发生，因此要想判断劫持行为究竟最终应该以何种罪名定罪则比较困难。而在司法实践的具体定罪争议中，“破坏”的行为方式与“非法控制”的行为方式在实践中常常交织在一起，会更加难以区分，这主要体现在一方面，为了不正当地控制计算机信息系统，行为人完全有可能采取修改、增加、干扰、删除系统内的功能和数据等多种会影响系统正常运行的行为方式来实现自己对计算机信息系统的排他性控制。另一方面，当行为人通过篡改原权利人的相关信息系统中的账户或密码来完全控制该计算机信息系统时，这种表现出来的未经原权利人许可擅自修改账户和密码等其他数据信息的行为，通常也是实践中被认定为实施破坏计算机信息系统犯罪的法定行为类型之一。鉴于此可以认为，实践中非法控制计算机信息系统罪和破坏计算机信息系统罪在客观的行为表现方式上可能是相似的甚至是相同的，因此造成了两者在司法实践的适用上难以区分的困境。

2. 相关计算机犯罪立法规定粗疏

目前司法实践对于流量劫持主要采用以计算机类犯罪进行定罪的思路。而从立法的发展脉络和演进来看，破坏计算机信息系统罪是 1997 年刑法设立并开始规制的罪名，而非法控制计算机系统罪是应时代发展以及社会回应需要通过《刑法修正案（七）》新追加的罪名，其与非法获取计算机信息系统数据罪相并列共同被规定在《刑法》第 285 条之中，该条款的设立一方面是为了弥补第 284 条非

[26] 参见孙道萃：《“流量劫持”的刑法规制和完善》，载《中国检察官》2016 年第 4 期，第 76 页。

法侵入计算机信息系统罪中规制的特定计算机信息系统类型之外的保护不足的问题，同时也是为了补充破坏计算机信息系统罪随着信息技术的发展运用所暴露出的规制漏洞，因此两罪在设立之初其行为方式和所规制的犯罪类型应当是有着明显区分的。通过对二罪刑法规范叙述的比较可以发现立法对二罪的规定均较为粗疏。特别是非法控制计算机系统罪的罪状规定较为简化，立法对于什么是“非法控制”没有进行详细的规定，司法解释也焉语不详，因此在实践中认定“非法控制”的状况稍显混乱，甚至有的法院形成了非法控制就是破坏的错误认知，这也就直接导致了实践情况中非法控制计算机信息系统罪与破坏计算机信息系统罪之间的界限不明的问题。正因为立法对“破坏”和“非法控制”行为的界限规定得不够清晰，因而出现了司法竞合现象。就上文引用论述的案例一和案例二的裁判结果其实各有其合理性：一方面，DNS 型流量劫持其本身既符合非法控制行为的危害特征，也同时具备破坏行为的内在体现。而从“非法控制”行为与“破坏”行为的语意逻辑表现来看，二者应当是特殊与一般或者说是被包含与包含的关系，非法控制可以被视为是破坏行为的一种特别具体体现，而从特别优于一般的定罪逻辑来看，将流量劫持定为非法控制计算机信息系统罪并无差错；另一方面，立法中破坏计算机信息系统罪整体的法定刑显然比非法控制计算机信息系统罪更高，按照理论和实践中对于二罪想象竞合的“从一重处断”的一般处断原则，以破坏计算机信息系统罪规制流量劫持显得更为合理。因此，立法规定的缺憾导致司法实践对于流量劫持的规制出现竞合，此难题将导致此类同案不同判的现象无法被合理应答的困境。

3. 理论界对流量劫持侵害法益的认识侧重不同

通过上文对理论界争议焦点的梳理可以很明显地发现学者们之所以对流量劫持有不同的定罪路径，关键在于其侧重关注和保护的法益不同。持计算机犯罪规制思路的学者们更多着眼于流量劫持行为本身及其破坏结果，即主要看到了流量劫持技术本身对计算机信息系统的正常运行以及相关功能的干扰与破坏，因此侧重于对计算机信息系统自身运行安全的维护；而持财产犯罪规制思路的学者们则更关注到流量劫持行为发生的根源和目的在于恶意转移目标网站的网站流量，而网站流量在市场上具有巨大的财产价值，同时也是网络运营商盈利的重要来源，因此其侧重于对受害网络运营商以及网络用户相关合法权益的保护。正因为

流量劫持侵害的是多重法益，因此当学者们所侧重认识的法益不同时，其定罪的角度和思路自然而然会发生分歧和偏差。

三、 流量劫持行为刑事定罪路径选择

这一部分内容将针对实务界和理论界关于流量劫持定罪思路的分歧进行评价与比较，综合分析各种定罪思路的内在问题以及优缺点，最后提出对于流量劫持的定罪意见。

（一） 以计算机犯罪定罪路径之具体证成

1.流量劫持侵害计算机犯罪相关保护法益

既然司法实践普遍选择采用计算机犯罪规制流量劫持必然有其合理性，在此基础上首先需要讨论的问题必然是法益。以实践多数案例所指向的定罪类型——DNS 流量劫持为例，DNS 流量劫持的社会危害性较重，侵害的是多元法益，而技术实施之时最先冲击的必然是计算机信息系统，因此其会对计算机信息系统的安全运行造成损害，这也是诸多案例裁判最主要的裁判要点。而刑法分则将与计算机信息系统相关的犯罪虽然设立在第六章“妨害社会管理秩序罪”，对应到第六章中，刑法规定此类犯罪所保护的法益是国家对计算机信息系统安全的管理秩序，[27]但并非意味着这与 DNS 流量劫持所侵害的法益毫无关系，个罪对法益的保护相对具体且联系紧密。以实践中定罪较多的非法控制计算机信息系统罪与破坏计算机信息系统罪为例，非法控制计算机信息系统罪按照通说其保护的法益是计算机信息系统的安全，破坏计算机信息系统罪保护的法益是国家对计算机信息系统的安全运行管理制度和计算机信息系统的所有人与合法用户的合法权益。[28]可以看出，非法控制计算机信息系统罪的保护法益与 DNS 流量劫持所直接侵害的法益契合，而破坏计算机信息系统罪的保护法益也与之紧密相关，DNS 流量劫持确实也会对系统的所有人及用户的合法权益造成威胁，因此采用计算机犯罪对 DNS 流量劫持进行规制，可以保护大多数法益免受侵害。

[27] 参见王作富主编：《刑法分则实务研究（中）》，中国方正出版社 2009 年版，第 1200 页。
[28] 参见高铭暄、马克昌主编：《刑法学（第十版）》，北京大学出版社、高等教育出版社 2022 年版，第 540-541 页。

2. 适用破坏计算机信息系统罪判断

通过对破坏计算机信息系统罪的规范解读可以发现我国《刑法》第 286 条主要限制三种破坏行为方式：[29]

第一类概括来说是删、改、增、干扰计算机信息系统功能的行为，这种类型的破坏行为比较常见，实践中以 DNS 劫持情况为主。以李某案为例[30]，案例中所指向的行为实质上是对计算机系统功能的修改和干扰，符合第一种行为类型的规定。[31]另外，这里的“计算机信息系统”根据《计算机信息系统安全保护条例》（以下简称《条例》）的规定也有一定的限定和明确[32]，不可随意扩大其解释范围，而根据《条例》的规定，计算机信息系统要素相对广泛甚至包括了系统的使用者，但是本罪的犯罪对象根据刑法规定应当只涵盖计算机信息系统中的软件、信息数据和应用程序，对除此之外的计算机信息系统要素进行侵犯的，不应当构成本罪。[33]

第二类主要是删、改计算机信息系统存储、处理或传输的数据和应用程序，增加操作的行为。例如，在最高人民检察院的指导案例“李某等人计算机信息系统破坏案”的判决中曾强调：“假冒购物网站的消费者身份进入相关网站内部的评价系统删除或者修改消费者的购物评价是修改计算机信息系统内部存储数据的操作，应确认为是破坏计算机信息系统的行为。”[34]与第一种类型相比，虽然操作方法均是删除、修改和增加操作，但两者所指向对象大有不同。在第一种类型中删除、修改和增加的是计算机信息系统的功能，因此系统被破坏，无法正常运转。需要特别注意的是,该类型行为表现中行为人删除、修改和增加的是存储在计算机系统中的数据和应用程序，没有明文要求必须破坏系统功能。另外，通

---

[29] 《刑法》第二百八十六条 【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。

[30] 该案判决指明“修改域名分析服务器的运作方向，强迫用户离开想要进行访问的网站或网页而进入到由侵入者恶意设定的网站或网页，是典型的域名劫持行为”。行为人使用恶意代码更改目标网站的域名分析服务器，目标访问网站被恶意解读为其他 IP 地址，使得目标网站的服务功能无法正常运行。

[31] 参见最高人民检察院第 33 号指导性案例——李丙龙破坏计算机信息系统案。

[32] 国务院关于《计算机信息系统安全保护条例》第二条第一款

计算机信息系统由计算机及其相关设备、设施（包括网络）构成，按照一定的应用目标和规则收集信息，加工、存储、传输、指进行检索等处理的人机系统。

[33] 参见王作富主编：《刑法分则实务研究（中）》，中国方正出版社 2009 年版，第 1209 页。

[34] 参见李骏杰等破坏计算机信息系统案，最高人民检察院第 34 号指导案例（2017 年）。

过对实践案例的分析和总结，发现行为人选择直接删除、修改或增加系统数据的情形较为普遍，而选择直接破坏应用程序的情况则比较少见。从技术实现角度来看，直接对数据进行操作比破坏一款相对完整的应用程序较为容易实现。但从立法文义来看，“数据”和“应用程序”均可以成为本罪的犯罪对象，二者是“或”的关系而非“且”的关系，也就是说，行为人在二者中选择其一进行破坏就可以构罪。[35]这样才能实现对数据和应用程序的周延高效保护。

第三类是故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行的行为。这种类型与前两种类型相比，认定难度低，实践中争论较少，也比较容易判断制作电脑病毒等破坏性程序，且通过相关司法解释规定了如何判定实践中“计算机病毒等破坏性程序”的不同情形，[36]并强调了如何认定实践中造成的严重后果。此外在特殊情形下，如果程序的设计比较复杂，实践中一般难以确定的，还可以委托相关技术部门进行检验。[37]

必须强调的是，根据刑法规定，实施上述几种破坏计算机信息系统的行为，要求只有在产生严重后果的情形下才能构成本罪，因此，本罪是典型的结果犯的构造。同时必须明确，第一类和第三类破坏行为均要求对计算机信息的功能施加作用，即造成系统不能运行或者不能正常运行，虽然立法在第二类破坏行为中并未对此进行明确规定，但是应当认为破坏计算机信息系统罪的三类“破坏”行为均应该达到“造成计算机信息系统不能正常运行或不能按照设计要求运行”的后果。因为立法既然将这三类行为类型并列，间接反映同一犯罪的多种表现形式的社会危害性程度是相当的。至于为何在第二类中未明确写明对计算机信息系统功能施加影响的要求，或许立法者有自己的考量。而且司法实践对此种情况也进行了回应，最高人民法院第 145 号指导性案例明确表示“通过修改、增加计算机信息系统数据，未造成系统功能实质性破坏或者不能正常运行的，不应当认定为破

[35] 参见何帆：《刑法注释书》（第二版），中国民主法制出版社 2021 年版，第 776 页。

[36] 《最高人民法院、最高人民检察院危害计算机信息系统安全刑事案件应用法律问题的解释》第五条

具有下列情形之一的程序，应当认定为刑法第二百八十六条第三款规定的“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，并破坏计算机系统功能、数据或者应用程序的程序。

[37] 实践中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。

坏计算机信息系统罪”[38]。因此应当认为计算机信息系统功能的影响破坏与否是破坏计算机信息系统罪三种行为类型均需具备的结果要素。[39]

综上所述，针对 DNS 流量劫持，实践中常见的是破坏计算机信息系统罪的第一种行为类型，即通过恶意修改 DNS 服务器所指向的域名，对服务器系统的域名解析功能造成损毁，造成该系统无法正常运行。

3. 适用非法控制计算机信息系统罪判断

回归到刑法对于非法控制计算机信息系统罪的规定，我国《刑法》第二百八十五第二款对该罪仅仅通过简单罪状的形式予以表述[40]，因此重点在于对“非法控制”作何种理解。对于如何解读这里的非法控制，学术界有不同的观点。高铭暄学者认为，非法控制是指“未经许可，违反计算机信息系统原用户意愿操作使用该系统，掌控系统活动的行为”。[41]在这里，高学者强调的是，非法控制首先违反了合法用户的意愿，即“违法性”。还有一些学者认为，非法控制可以解释为“通过技术手段下达指令，将用户的计算机信息系统置于行为人的控制之下，为行为人控制和使用”，即“可控性”。[42]该观点强调了入侵者对计算机信息系统享受的控制支配地位，与立法者的观点“所谓不法控制，是指通过各种技术手段将他人的计算机信息系统置于自己的控制之下，按照自己发出的相关指令程序，完成相应的操控”[43]具有相似性。叶良芳学者还对非法控制进行了更细致的区分。她主张：“根据控制程度的不同，非法控制可以分为全部控制和部分控制。”[44]该主张中的全部控制是指计算机信息系统完全被入侵者绑架，用户也完全失去操作计算机信息系统功能的自由；所谓部分控制，是指用户拥有一部分操作计算机信息系统的权限，实践中大多数情况是部分控制。可见，叶良芳学者在非法控

---

[38] 参见张竣杰等非法控制计算机信息系统案，最高人民法院指导案例 145 号（2018 年）。

[39] 参见阎二鹏：《干扰型破坏计算机信息系统罪的司法认定》，载《中国刑事法杂志》2022 年第 3 期，第 127—128 页。

[40] 《刑法》第二百八十五第二款

违反国家规定，侵入前款规定以外的计算机信息系统对该计算机信息系统实施非法控制，情节严重的行为。这里的“前款”指的是“非法侵入计算机信息系统罪”，因非法侵入计算机信息系统罪所特殊保护的是国家事务、国防建设、尖端科学计算领域的计算机信息系统，故非法控制计算机信息系统罪所保护的是此三种类型之外的计算机信息系统。

[41] 高铭暄： 《中华人民共和国刑法的孕育诞生和发展完善》，北京大学出版社 2012 年版，第 510 页。

[42] 参见肖怡：《流量劫持行为在计算机犯罪中的定性研究》，载《首均师范大学学报（社会科学版）》2020 年第 1 期，第 37-44 页。

[43] 参见全国人大常委会法制工作委员会刑法室编:《〈中华人民共和国刑法〉条文说明、立法理由和相关规定》，北京大学出版社，2009 年，第 591 页。

[44] 叶良芳：《刑法教义学视角下流量劫持行为的性质探究》,载《中州学刊》2016 年第 8 期，第 45-49 页。

制的基本概念的基础上，根据行为人的控制程度，结合实践情况，对非法控制的种类进行了更加细致完善的划分，同时也指出了非法控制行为的本质也即侵入者的目的是实现对系统的排他使用。

上述观点侧重于“非法控制”的行为目的以及行为特点的剖析，但仍然无法解决实践中的某些难题。在指导案例中，用户完全不知道傅某等人通过恶意软件和程序侵入用户的 DNS 服务器的事实，被告人此时在未经用户允许的情况下完全控制了服务器的使用，并因此恶意改变了 DNS 服务器的解析结果以实现自己的非法目的，但法院没有根据上述论证的非法控制的行为特点将其认定为“非法控制”行为而是将其认定为“破坏”行为。在案例二中，施某本来拥有对计算机信息系统的合法控制权，但由于其滥用权力进入系统，也是对系统实施了控制并私自改动 DNS 相关数据信息，造成 DNS 系统正常的域名解析功能无法发挥作用，却被认定为“非法控制”，此为实践情形中值得深思和解释的地方，为何同一种行为类型却有着不同的司法定性结果。相关立法似乎忽视了对这些概念的定义和区分，但相关司法解释反映了司法机关对此类情况的认定思路和宗旨，即行为人只要非法取得对计算机信息系统的控制权则构成非法控制，[45]但是根据司法解释的精神实质，此种认定思路过于直接和简洁。

通过案例检索可以发现，实践中的非法控制计算机信息系统案件以利用木马程序抓取肉鸡类为主，即通过将木马程序或者黑客软件等植入他人的计算机从而实现对计算机的远程控制，进而实施流量出售、分布式拒绝服务攻击和违法广告推广获利等行为。以余某案为例，其就是通过技术手段实现对目标网站后台的控制，在目标网页上植入广告进而牟利。[46]再结合实践具体情形，本文认为“非法控制”可以理解为在行为人没有获得网络用户或网络运营商的合法授权或者超越授权的情况下，擅自进入系统，控制系统的运行和使用，这里的控制更强调一种

[45] 《最高人民法院、最高人民检察院关于处理危害计算机信息系统安全的刑事案件的法律若干问题的解释》第七条第一款

“明知是非法获取计算机信息系统数据犯罪所获取的数据、非法控制计算机信息系统犯罪所获取的计算机信息系统控制权，而予以转移、收购、代为销售或者以其他方法掩饰、隐瞒，违法所得五千元以上的，应当依照刑法第三百一十二条第一款的规定，以掩饰、隐瞒犯罪所得罪定罪处罚。”

[46] 参见余某非法控制计算机信息系统案，江苏省海安县人民法院刑事一审判决书，（2018）苏 0621 刑初 60 号。

本案中，被告人余某通过软件批量扫描目标网站系统的漏洞，再通过木马程序，设置密码，从而获得目标网站后台的控制权（即称 webshell 链接），再将目标网站所对应的 webshell 链接导入 XISE 软件，在目标网站页面上植入相应的广告，并从中牟利或将这些各不相同 webshell 链接出售给他人从中牟利。被告人余某犯非法控制计算机信息系统罪。

行为产生的事实状态而非结果，即行为人未经许可通过删、改、增系统数据等手段，达到对系统完全支配或部分支配的程度，而这一控制行为造成的后果是使系统按照行为人的重新设定或意愿运作，至于是否要实际或者直接造成破坏或妨碍计算机信息系统的正常运行的后果，是否必须对系统功能产生影响并不是“非法控制”行为所关心的重点。[47]事实上，行为人此时构成非法控制计算机信息系统罪已经没有争议，关键是行为人未经用户许可恶意修改用户路由器内的 DNS 设置，修改域名的解析配置，当然属于立法规定中对计算机信息系统数据及功能的修改，既然如此，施某的行为又是否满足”破坏”行为的特征而被评价为破坏计算机信息系统呢？这两个罪名之间又存在什么关联？这是需要进一步分析的。

4. “破坏”与“非法控制”的行为辨析

基于以上论证可以明晰，实践中两罪之所以会发生认定争议，关键在于立法对于“破坏行为”与“非法控制行为”的本质和构造未进行明确的规定和辨析，以及实务部门忽视了对破坏计算机信息系统罪结果要素的考察。然而事实上，“破坏”与“非法控制”并非完全对立也并非是法条竞合的关系，二者存在一种辩证统一的关系，既相互区分又相互联系。在此本文将从行为本质和行为构造两方面对“破坏”与非法控制进行区分，同时指出二者各自的判断要点。

（1） 行为本质辨析

从立法原意分析，“破坏计算机信息系统”的本质是给系统的功能带来实质性的损伤，使其不能正常工作。“非法控制计算机信息系统”的本质是意图排除计算机信息系统的原权利人对系统的控制和使用权利，使系统不能按照原权利人的意愿开展工作和运行。因此，该罪客观上在实践中经常表现为行为人未经授权或超越权限擅自利用技术控制计算机信息系统。而破坏计算机信息系统在实践中更多表现为行为人通过相关技术直接破坏计算机信息系统的硬软件设施，影响其相关功能，导致计算机信息系统不能正常工作。简言之，“非法控制”从保护计算机信息系统原权利人控制权的角度，强调行为人对计算机信息系统的非法操纵状态和权限剥夺；而“破坏”着重于保护计算机信息系统的安全运行，强调了行为人对计算机信息系统的功能破坏和无法正常运行损害，此乃二者在行为本质上

[47] 参见叶良芳：《刑法教义学视角下流量劫持行为的性质探究》，载《中州学刊》2016 年第 8 期，第 45-49 页。