第 3 章

网络犯罪的法律规制

本章学习目标

- 境外国家网络犯罪的法律规制
- 我国网络犯罪的法律规制
- 计算机网络作为目标的法律规制
- 计算机网络作为工具的法律规制
- 网络犯罪的刑事程序法律规制
- 网络犯罪的电子数据法律规制

法律规制是依法惩治网络犯罪的前提和基础。在打击网络犯罪时，各国国情以及所要规范的对象会成为影响法律规制的重要因素。在我国法律层面，对网络犯罪的法律规制的理解需要从实体法规范、程序法规范和证据规则三个角度进行。对于网络犯罪的立法，我国设立刑法、刑事诉讼法、司法解释以及规范性文件，这些规范共同构建起我国网络犯罪的法律规制体系。

本章通过对各国立法的背景进行介绍，简要概括网络犯罪的法律规制的模式选择，阐述我国各项网络犯罪的相关法律法规及有关规定，重点解读立法过程和立法意图，以帮助读者系统了解并掌握我国网络犯罪的法律规制体系。

3.1 网络犯罪的法律规制概述

世界各国的主要法律体系主要分为大陆法系和英美法系。大陆法系一直以来都有以成文法立法的传统，针对法律所调整的对象不同，划分不同的部门法，各部门法之间相互协助、相互依存，共同形成统一的、完整的立法体系。英美法系虽然也有成文法，但是需要判例来充实实体法的内容，实质上依然是判例法。法官审理案件时，并不是依据成文法法条进行演绎，而是先前的判例和相关的法律精神。在这种模式下，英美法系经常会根据不同的情况产生新的判例或者指定特别法，以更新或者丰富法律规范体系。

我国属于大陆法系国家，刑事立法在总体上也是遵循成文法的立法传统。虽然各级法院也会针对办案实践定期出台指导性判例，但是这些判例的主要作用是为了实现各地以及各级法院之间对法律适用的统一性，指导各级法院正确理解和适用相关法律法规，而非英美

法系国家的“判例法”性质。我国的网络犯罪的法律规制属于刑事立法的范畴，也是遵循成文法的立法模式。因此在办理网络犯罪案件时，只能以各项成文法作为法律依据。相关法律体系的完善，也是以制定和修改成文法为途径。

3.1.1 境外网络犯罪的法律规制

网络无国界，各国面对的网络犯罪形式近似。因此，在当今时代背景下，网络犯罪的法律规制已然成为世界各国的共同话题，各国政府都制定了针对网络犯罪的法律法规。这些法律法规有些是以专门法形式出现，有些是以原有法律增加条款的形式出现。究竟哪种形式能更有效地遏制网络犯罪，至今还未有一个定论。如同网络发展方兴未艾，网络犯罪的法律规制也处于不停的发展过程中。

1. 国际公约

在20世纪80年代，欧洲理事会开始呼吁要更多地关注黑客行为和计算机相关犯罪给国际社会所带来的威胁，1997年欧洲理事会建立了网络犯罪专家委员会，并开始起草《网络犯罪公约》(以下简称《公约》)，《公约》涵盖刑事实体法、程序法和国际协作等内容，在2001年11月8日获欧洲理事会部长委员会通过，26个欧盟成员国以及美国、加拿大、日本和南非等30个国家在布达佩斯签署。按照《网络犯罪公约》的规定，网络犯罪分为四类，具体包括：纯粹的网络犯罪，即以非法入侵、非法干预、删改数据、删改系统、滥用设备等方式实施的损害互联网通信秘密性、完整性和可用性的犯罪行为；通过互联网实施的诈骗、伪造等传统的犯罪行为；通过互联网传播非法内容的犯罪行为；通过互联网实施的知识产权犯罪行为。

《公约》从破坏计算机数据和系统的保密性、完整性和可用性的犯罪、与计算机相关的犯罪和与内容相关的犯罪等几个方面，规定了各成员国打击信息网络犯罪的立法义务，是世界上最早也是目前影响范围最广、最重要的打击网络犯罪的国际公约，目前已经成为世界主要国家的立法范本。

2009年4月20日，欧盟在捷克首都布拉格通过《布拉格宣言》，要求各成员国加强协调，促进打击网络犯罪的国际合作，保证互联网的安全。

2011年5月，由“美、英、德、法、意、加、日和俄罗斯”组成的“八国集团”通过《多维尔宣言》，强调互联网自由、开放和同名，尊重公民隐私和保护知识产权，维护网络安全和打击网络犯罪。

2. 美国

互联网最早发展起来的美国是面临网络犯罪冲击最早，也是最先制定网络犯罪法律规制的国家。作为一项新兴事物，美国是需要制定一套特殊的法律，还是对现实空间的法律作一些调整？曾经引起了很大的争议[①]。对此，法官弗兰克·伊斯特布鲁克曾经指出：正如

① 此争议也广泛地发生于世界各国网络犯罪法律制定过程中。

没有必要制定“马法”(Law of House)一样,也没有必要制订“网络法”[①]。这就是著名的“马法非法[②]”之争。1997 年 10 月,美国《时代》周刊以“隐私之死”作为封面标题指出了信息时代隐私保护的重大难题。网络犯罪已经给美国社会带来了巨大的危害,立法的呼声占据上风。“马法非法”之争的结论显而易见。

1970 年,美国颁布了《金融秘密权利法》,对于金融行业保管的信息数据进行了规范。1977 年制定《联邦计算机系统保护法》,首次将计算机系统纳入法律。1978 年,美国弗罗里达州制定了第一部计算机犯罪法,规定了计算机犯罪的具体形式。随后,美国各州相继颁布了计算机犯罪法。1984 年 1 月,美国修改了刑法典,在第 18 篇第 47 章中规定计算机犯罪,其中具体包括下列行为:“(1)自计算机取得机密情报罪;(2)自计算机取得金钱或信用情报罪;(3)妨害联邦计算机系统罪。”[③]

1984 年 10 月,里根总统签署了美国第一部联邦计算机犯罪的成文法《伪装进入设施和计算机欺诈及滥用法》;1986 年又颁布了《计算机诈骗和滥用法》,将非法活动分为四类,分别是:“(1)任何无授权的读取系统,尤其是读取绝密文件或机密政府文件;(2)非法读取财物方面信息;(3)任何无授权的读取任何美国政府的计算机;(4)有目的地买卖非法的信息数据。”[④]1994 年,美国议会通过了《计算机滥用修正法案》。

在最初,美国在网络犯罪方面的立法是将重点放在未经许可而故意进入联邦计算机的行为上。1993 年以后,则扩大了网络犯罪的责任范围,并开始为网络犯罪的受害者提供民事补偿。自此之后,美国开始不断构建和完善网络犯罪的法律规制的体系并始终走在世界前列。

到目前为止,美国联邦立法出台的涉及打击网络犯罪的法案共包括以下几项:《美国联邦计算机欺诈与滥用法案》(Computer Fraud and Abuse Act. 18 USC 1001 note),该法案旨在对利用计算机和接入设备的欺诈及相关行为提供额外的惩罚;《美国联邦计算机安全法案》(Computer Security Act of 1987. PL 100—235. January 8, 1988, 101 Stat 1724),该法案旨在为国家标准局提供计算机程序的标准,为政府计算机网络提供安全保障,为管理、操作、使用联邦计算机系统的安全事务人员提供培训以及其他目的;《美国联邦禁止电子盗窃法案》(No Electronic Theft (NET) Act. 105th Congress—First Session Convening January 7,1997),该法案的目的在于修订美国法典第 17 部和第 18 部,通过修订刑法来给予

---

① Frank Easterbrook. Cyber and The Law of House. University of Chicago law forum, 1996: 207

② 美国联邦上诉法院的法官弗兰克·伊斯特布鲁克提出“马法非法”。他认为,网络法的意义就同“马法”——即关于马的法律——差不多。“马法”是一个必要的法律部门吗?显然是否定的。马的所有权问题由财产法规范,马的买卖问题由交易法管束,马踢伤人分清责任要找侵权法,马的品种、许可证、估价和治病均有相应部门法处理……如果有人企图将之汇集为一部“马法”,那将极大地损害法律体系的统一性。他指出,Internet 引起的法律问题具有同样的性质。网络空间的许多行为很容易归入传统法律体系加以调整。为了网络而人为地裁减现行法律、创制网络法,不过是别出心裁,没有任何积极意义。

③ 刘广三. 计算机犯罪论. 北京:中国人民大学出版社 1999: 140-142

④ [英]尼尔·巴雷特. 数字化犯罪. 北京:郝海洋,译. 沈阳:辽宁教育出版社,1998: 113

著作权更大的保护；《美国联邦禁止网上攻击者法案》(Deleting Online Predators Act of 2006)，该法案旨在修改 1934 年通信法，以保护在商业社交网站和聊天室的未成年人利益；《美国联邦非法互联网赌博执行法案》(Unlawful Internet Gambling Enforcement Act of 2006)，该法案旨在加强联邦对非法互联网赌博的打击力度。在《美国联邦刑法与刑事诉讼法》(United States Crimes and Crininal Procedure)的“刑法”部分，也有多项规定与网络犯罪行为有关。

3. 欧洲国家

欧盟的多数国家，自 20 世纪八九十年代起就开始针对其国内刑法是否能够适用于信息网络技术实施的新型犯罪进行审视和研究，并对其刑法进行适当的修改、发展和补充。其中，法国、德国、丹麦、奥地利、瑞典等国分别不同程度地对其本国刑法的罪名体系进行了修改；而英国、葡萄牙、西班牙等国则只是在原有刑法基础上对计算机犯罪进行了增补。总体来讲，欧洲大多数国家实际上已经具备了比较完整的网络犯罪罪名体系。

例如，德国在 1986 年 8 月 1 日对其刑法进行了修正，加入了有关防治计算机犯罪的各项规定，主要包括计算机欺诈罪、资料伪造罪、刺探资料罪、变更资料罪、计算机破坏罪等。2007 年 8 月 7 日德国“为打击计算机犯罪的《刑法》第 41 修正案”获得通过，该修正案完成了欧洲理事会《关于网络犯罪的公约》和欧盟委员会《关于打击计算机犯罪的框架决议》在德国刑法中的移植。《修正案》生效后德国网络犯罪立法对侵犯计算机数据和信息系统安全的犯罪规定了窥探数据、拦截数据、预备窥探和拦截数据、变更数据以及破坏计算机五个方面的行为与罪名。德国没有一味追求最高标准的网络犯罪立法，而是在国际公约允许的范围内，根据本国网络犯罪状况和本国刑事政策进行修改网络犯罪立法，其突出的特点是轻罪处罚轻缓，重罪处罚严厉。作为德国刑法的一贯特点，《修正案》对各罪罪状的描述和使用术语规定得十分明确和准确，区分不同危害程度的犯罪情节并设置差别化的刑罚，这些都是德国网络犯罪立法值得借鉴之处①。

欧洲另一个比较有代表性的国家是法国。现行《法国刑法典》于 1994 年 3 月 1 日生效，其中第 3 卷第 3 编第 3 章专章规定了“侵犯资料自动处理系统罪”，分别对侵害计算机信息系统、侵害计算机存储数据以及相关特殊行为的处罚进行了规定。其中，对于针对计算机信息系统实施的犯罪，《法国刑法典》用比较系统的篇幅对非法侵入计算机信息系统、破坏计算机信息系统的行为进行了规定，具体包括“非法侵入系统或者在系统中非法停留”(第 323-1 条第 1 款)和“破坏计算机信息系统”(第 323-1 条第 2 款)两类犯罪行为。此外，对于针对计算机存储数据实施的犯罪，《法国刑法典》将这一类型犯罪分为两种情况分别加以规定，具体为“破坏存储数据犯罪”(第 323-1 条第 2 款)和“非法输入数据犯罪”(第 323-3 条)。同时，该法还通过特殊条款，对网络犯罪的组织形态、犯罪停止形态的处罚作出了规定，如对网络犯罪未遂的处罚、对网络犯罪集团的处罚等。

---

① 皮勇. 论欧洲刑事法一体化背景下的德国网络犯罪立法. 中外法学，2011，23(5)：1060

4. 亚洲国家

亚洲拥有世界上最多的网民，网络犯罪也因此成为困扰亚洲各国的难题之一。日本、印度、韩国等亚洲各国和地区都纷纷尝试进行网络犯罪的法律规制体系的构建和完善。

1）日本

作为大陆法系的代表性国家，日本在关于网络犯罪的立法模式与内容上基本沿袭了德国的相关立法经验。1987 年日本通过刑法修正案出台了第一部关于网络犯罪的规范，对于“电磁记录”“文书”等信息时代的新概念进行界定。此次修改，奠定了日本关于网络犯罪的法律规制的罪名体系。在内容上，日本刑法典中关于网络犯罪的罪名主要包括：损害电子计算机系统等妨害计算机系统罪[①]；毁弃文书罪；非法制作和提供电磁记录罪；计算机欺诈罪等罪名。

2）韩国

在当前的韩国刑法中，网络不良行为的罪名主要有第 316 条第 2 项“侵犯隐私罪”、第 314 条第 2 项“电脑等业务妨害罪”、第 366 条“电脑损坏罪”、第 347 条“电脑等使用欺诈罪”。

除刑法之外，韩国国会于 2000 年 12 月通过了《信息通信的基本保护法》(2001 年 7 月 1 日开始实行)，该法的出现主要是针对黑客、病毒等电子侵害行为在网上肆虐的问题，而当时的处理措施缺乏综合性、系统性。

此后，2008 年韩国修订了《信息通信网的利用促进以及信息保护等相关法》(简称《信息通信网法》)，开始对与信息通信网相关的网络恐怖行为进行定罪，主要追究那些“没有正当的接近权限或超出已有的接近权限侵入信息通信网”的行为，具体来说，可以构成以下几项罪名：信息通信网侵入罪、信息通信网隐私侵害罪、信息通信网信息毁损罪、恶性程序传播罪、个人信息无端使用罪、网络淫秽物以及信息通信网淫秽符号的传播罪、违反青少年有害媒体物标示罪、信息通信网利用的公众心理造成罪、网络公害犯罪、网络名誉损害罪、ID 盗用罪等。

3.1.2　中国网络犯罪的法律规制

法律是社会关系的调节器，这一点对网络社会也同样适用。完善、合理的法律规范可以有效地预防和打击网络犯罪行为，保障国家和公民的合法权益，维护网络社会的正常秩序。

1. 中国大陆

1980—1997 年，这一阶段属于计算机发展阶段。1981 年公安部成立了计算机安全监察机构，并着手开始制定有关计算机安全方面的法律法规和规章制度。1986 年 4 月开始草拟《中华人民共和国计算机信息系统安全保护条例》(征求意见稿)。1989 年，在重庆发现了首例计算机病毒，随后公安部发布了《计算机病毒控制规定(草案)》，并开始推行“计算机病毒

① 损害电子计算机系统等妨害计算机系统罪后来被指责过于宽泛而被修改。

研究和计算机病毒防治产品销售许可证”制度。1991 年 5 月 24 日，国务院第八十三次常委会依照《中华人民共和国著作权法》的规定制定并通过了《计算机软件保护条例》，这是我国第一部有关计算机的法律。1992 年 4 月 6 日，机械电子工业部发布了《计算机软件著作权登记办法》，规定了计算机软件著作权管理的细则。1994 年 2 月 18 日，国务院发布了《中华人民共和国计算机信息系统安全保护条例》，为保护计算机信息系统的安全，促进计算机的应用和发展，保障经济建设的顺利进行提供了法律保障。1996 年 2 月 1 日国务院发布了《中华人民共和国计算机信息网络国际联网管理暂行规定》，提出了对国际联网实行统筹规划、统一标准、分级管理、促进发展的基本原则。

1997 年 10 月 1 日，我国对《刑法》进行修改，第一次增加了计算机犯罪的罪名，包括非法侵入计算机信息系统罪，破坏计算机系统功能罪，破坏计算机系统数据罪。这标志着我国对计算机及网络管理的法制体系建设进入了一个新的阶段。

2000 年，我国进一步加快了计算机与网络立法的步伐。为了规范电信市场秩序，维护电信用户和电信业务经营者的合法权益，保障电信网络信息的安全，促进电信事业的健康发展，国务院于 9 月 20 日通过了《中华人民共和国电信条例》。同年 10 月，为了加强对互联网内容服务的监督管理，防止有害信息危害社会，尤其是对国家安全、社会稳定和公共秩序造成危害，国务院专门起草了《关于维护网络安全和信息安全的决定(草案)》，并提请全国人大常委会审议。之后，为维护国家安全和社会稳定，保障网络安全，维护社会主义市场经济秩序和社会管理秩序，保护公民、法人和其他组织的合法权益等四个方面出发，国务院发布了《互联网信息服务管理办法》。2000 年 12 月 28 日，九届全国人大常委会第十九次会议表决通过《全国人民代表大会常务委员会关于维护互联网安全的决定》。自此掀开了我国在新世纪对计算机和网络加强立法的序幕。

2009 年 2 月 28 日，中华人民共和国第十一届全国人民代表大会常务委员会第七次会议审议通过《中华人民共和国刑法修正案(七)》(以下简称《刑法修正案(七)》或《修七》)，并于公布之日实施。《刑法修正案(七)》针对网络犯罪，增设非法获取计算机信息系统数据、控制计算机信息系统罪和提供侵入、非法控制计算机信息系统的程序、工具罪两项新的网络犯罪罪名。在《刑法修正案(七)》实施之后，最高人民法院、最高人民检察院于 2011 年 8 月 30 日，发布了《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》。《危害计算机信息系统安全犯罪解释》全面解释了危害计算机信息系统安全犯罪的法律适用问题，并且在诸多问题上对传统刑法理论进行了突破，解决了长期困扰司法实践的一系列突出问题。

2015 年 8 月 29 日，中华人民共和国第十二届全国人民代表大会常务委员会第十六次会议通过《中华人民共和国刑法修正案(九)》，自 2015 年 11 月 1 日起施行。《刑法修正案(九)》中关于网络犯罪相关内容做出多项重大修改，新增了网络犯罪预备行为，网络犯罪帮助行为，拒不履行信息网络安全管理义务等罪名，同时规定了网络犯罪的单位犯罪情形，利用信息网络传播虚假信息等内容。

在程序立法方面，针对刑事诉讼中办理网络犯罪案件的需要，也适时作出了相应的修改。2012 年 3 月 14 日第十一届全国人民代表大会第五次会议通过《关于修改〈中华人民共和国刑事诉讼法〉的决定》，并于 2013 年 1 月 1 日起实施，其中最重要的修改之一就是将电子数据正式列入法定的证据种类。2012 年 11 月 5 日，最高人民法院审判委员会第 1559 次会议通过了《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》，并自 2013 年 1 月 1 日起与新的《刑事诉讼法》同时实施。在新的《刑诉解释》中，对网络犯罪的犯罪地界定、电子数据证据的范畴和审查内容以及电子数据的排除规则等作出了明确规定。2014 年 5 月 6 日，最高人民法院、最高人民检察院、公安部印发了《关于办理网络违法犯罪案件适用刑事诉讼程序若干问题的意见》，针对公安机关、人民检察院、人民法院在办理网络犯罪案件程序上遇到的案件管辖不明确、跨地域取证困难、立案前可采取的侦查措施不明、电子数据取证程序有待规范等新情况、新问题出台了一系列明确意见，为依法惩治网络犯罪活动提供了有力的保障。

除了上述在实体法与程序法方面进行的立法活动之外，针对一些传统犯罪行为的网络化，我国还相继出台了一系列的司法解释，以解决办理此类案件时所面临的问题。其中主要包括：2004 年和 2007 年分别出台的《关于办理侵犯知识产权刑事案件具体应用法律若干问题的解释》和《关于办理侵犯知识产权刑事案件具体应用法律若干问题的解释(二)》两个司法解释；2004 年和 2010 年分别出台的《关于办理利用互联网移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释》和《关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释(二)》两个司法解释；2005 年出台的《关于办理赌博刑事案件具体应用法律若干问题的解释》；2010 年整治网络赌博专项行动期间，最高法、最高检、公安部专门联合出台的《关于办理网络赌博犯罪案件适用法律若干问题的意见》；2013 年 9 月 10 日出台的《最高人民法院、最高人民检察院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》等。

综上所述，自 20 世纪 80 年代以来，我国逐渐加强了针对计算机和网络安全的立法。特别是自 1997 年《刑法》修改增加网络犯罪相关罪名以来，在近二十年的时间里，我国在实体法和程序法两方面都逐步加强了关于网络犯罪的立法活动。随着刑事立法以及相关司法解释的出台与不断修改、完善，我国关于网络犯罪的立法体系正在逐渐形成之中。

然而，由于网络空间的虚拟性和复杂多样性，在打击和治理网络犯罪的司法实践中，仍然会有面临许多新的情况，使现有立法不可避免地表现出一定程度的滞后性。因此，在司法实践中，一方面要领会网络犯罪的法律规制的精神，适时调整对法律法规的理解，灵活运用，在依法办案的前提下有效使用现有的法律法规和司法解释；另一方面，执法部门要不断积累办案经验，总结在适用法律时所面临的具体困境，形成对立法效果的有益反馈，促进网络犯罪的法律规制的改进和完善。

2. 台湾地区

台湾地区刑法典将信息网络犯罪(台湾地区刑法典称“电脑犯罪”)单设一章,从非法入侵计算机信息系统或者相关设备,非法获取、破坏计算机信息系统或者相关设备数据,非法干扰计算机信息系统或者相关设备,制作专门用于信息网络犯罪的计算机程序等方面规定了网络犯罪的类型及处罚方法。

3. 香港地区

香港地区在立法方面,修订了原有的《电讯条例》《盗窃罪条例》和《刑事罪行条例》,增订了一些新罪行,扩大了原有条例的适用范围,形成了《电脑罪行条例》。另外,《电子交易条例》《版权条例》《个人资料条例》《证据条例》《防止儿童色情物品条例》《非应邀电子讯息条例》《赌博条例》《淫亵及不雅物品管制条例》等也都有关于网络犯罪打击的规定。

4. 澳门地区

澳门地区制定了《澳门特区打击电脑犯罪法》,作为打击网络犯罪的执法依据。

3.1.3 网络犯罪的立法模式

从目前制订和完善网络犯罪相关法律法规的角度看,主要有三种具体的立法模式可供选择。

1. 直接适用当前法律

将网络犯罪看成利用新工具的传统犯罪演变(Cyber as a Tool),适用现有的传统法律。这种模式主张不必重新立法,而是利用现有的法律来应对新的犯罪形式。因此,这种模式也被称为“保守的立法方式”。主张此立法模式的观点认为:网络虽然被称为虚拟的世界,被视作一个与现实有着众多差异的崭新空间,但归根结底它是现实生活的一种延伸。网络犯罪与现实生活中的社会犯罪并没有太大的差异,只不过犯罪分子使用的是一种新型的犯罪手段。所以“网络时代并不需要创造新的法律,唯一需要的是对现行法律的解释作更加明确的界定。”

2. 修正现行法律

这种模式主要通过修订既有的法律来实现,增加特别条款,使之适应信息化社会的需求,使其能够涵盖新出现的网络犯罪行为,如在犯罪对象中加入计算机系统、计算机网络等;或者是在对其他传统犯罪的规定中,将所列举的犯罪手段进一步扩充,在保持现有立法的稳定性和完整性基础上,把利用计算机和网络进行的犯罪行为也纳入其中。这种模式称为“渐进的立法方式”。主张这种模式的理由是:其一,计算机网络犯罪与现行刑法并非截然不能相通,其犯罪形态仍可纳入传统刑法体系中;其二,保持刑法的完整性,避免特别法多如牛毛;其三,适时增订足可维护刑法的妥当性与适应性,达到防治计算机网络犯罪的效果;其四,目前计算机网络科技尚未发展到极限,新方法或技术不断推出,专业化立法结果,法律本身势将时常修正。

3. 单独立法

由于网络犯罪在目的、方式、手段等方面所表现出的特殊性，现有立法的基本原则和基础理论都不能很好地适用，有必要单独针对网络犯罪的具体情况制定相应的法律规范。选择这种模式，就是要制定特别法，以单行法规的形式打击新出现的网络犯罪。在对网络犯罪全面认识的基础上，针对网络犯罪的特有形态、手段，对网络犯罪进行专法规定。这种模式称为“整体的立法方式”，这也是所有立法模式中实现难度最大的。主张采用这种立法模式的理由是：其一，对计算机网络犯罪的规范，例如定义、形态、特性、罪刑等，较为完整而有效；其二，易于修订；其三，较符合信息立法的精神。

对于网络犯罪而言，上述三种立法模式各有利弊。在具体选择的时候，不仅要根据本国现有立法体系和立法模式，选择与既有法律体系相兼容的模式；同时还要根据办理网络犯罪案件的实际情况，以适应司法实践的当时之需。

从各国立法的实践经验来看，第一种模式多为初期应对网络犯罪案件时的选择，因为受情势所迫，只能被动地依靠旧有法律对新的犯罪类型进行规范。例如在网络盗窃、网络诈骗等行为刚出现时，各国司法实践大多是以已有的盗窃罪和诈骗罪予以处罚。但是这种立法模式在面对网络犯罪带来的新特点时，就会有所局限，导致立法适用的障碍。例如 2005 年 12 月，深圳市在办理第一起 QQ 盗窃案件时，由于有关虚拟财产的认定没有相关法律的支持，无法使法院明确是否能以“盗窃罪”论处，因此最终选择以“侵犯通信自由罪”对相关行为进行定罪量刑。因此，在适用第一种立法模式时，为了克服其“被动性”给司法实践带来的桎梏，必须要适时对原有法律的适用作出恰当解释。并且，当对相关立法的经验积累和理论研究达到一定程度的时候，便应开始考虑选择第二种模式和第三种模式。

我国深受大陆法系传统影响。尽管重新制定单独的网络犯罪法律可以最大限度地覆盖网络空间的发展，但是我国信息产业起步较晚，发展程度参差不齐，因此目前在立法模式上采用的主要是第一种和第二种模式，即“保守的立法方式”和“渐进的立法方式”并存。

因此，侦查机关在考虑网络犯罪的定性，确立适用的刑法规范时，要注意以下两种情况：

一种是对于本质上与传统犯罪并无差异的网络犯罪，应考虑依然适用旧有法律，但可以针对新情况出台司法解释，以指明旧法在新情况下如何准确适用。例如，网络盗窃、网络赌博、网络诈骗等。这是依据第一种“保守的立法方式”。

另一种是针对纯粹的危害计算机信息系统安全类犯罪。旧有罪名不能涵盖此类新的犯罪类型。考虑到新设罪名依然遵循原有的刑法基本理论和基本原则，在刑法中单独进行修正，提出新的条款，仍属于原有刑法立法体系。这是依据第二种“渐进的立法方式”。例如我国在 1997 年修改的《刑法》以及后来的《刑法修正案(七)》和《刑法修正案(九)》两个修正案，在《刑法》中逐步加入了关于网络犯罪的条款，就是采用了这种立法模式。

随着我国网络经济在社会发展的比重增加，网络安全形势更加严峻。我国也根据形势的发展在酝酿推动《网络安全法》，在不久的将来，第三种模式“整体的立法方式”可能会出现，届时，我国在网络犯罪的法律规制可能会有一个巨大的飞跃，并对未来的立法产生深远

的影响。

3.2 计算机网络作为犯罪目标的法律规制

为了能够及时有效地打击网络犯罪，1997 年，《中华人民共和国刑法》增加第二百八十五条“非法侵入计算机信息系统罪”和第二百八十六条“破坏计算机信息系统罪[①]”。这是我国法律首次界定网络犯罪。2009 年《中华人民共和国刑法修正案(七)》在第二百八十五条新增两款规定：第二款罪名为“非法获取计算机信息系统数据、控制计算机信息系统罪”；第三款罪名为“提供侵入、非法控制计算机信息系统程序、工具罪[②]”。2015 年，《中华人民共和国刑法修正案(九)》在第二百八十六条中新增“拒不履行信息网络安全管理义务罪[③]”。上述网络犯罪可以统称为“危害计算机信息系统安全犯罪[④]”。

3.2.1 计算机网络作为目标的犯罪定性

根据《中华人民共和国刑法》的规定，对于计算机网络作为目标的犯罪活动主要以如下几项罪名约束。

第一，非法侵入计算机信息系统罪。《刑法》第二百八十五条第一款规定：“违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。”本罪是 1997 年《刑法》修改时就设立的罪名。

第二，非法获取计算机信息系统数据、控制计算机信息系统罪。《刑法》第二百八十五条第二款规定：“违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。”本罪是《刑法修正案(七)》中增设的罪名。

第三，提供侵入、非法控制计算机信息系统程序、工具罪。《刑法》第二百八十五条第三款规定：“提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，情节严重的，依照前款的规定处罚。”本罪是《刑法修正案(七)》中增设的罪名。

第四，破坏计算机信息系统罪。《刑法》第二百八十六条规定：“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

---

① 《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》。

② 《最高人民法院、最高人民检察院关于执行＜中华人民共和国刑法＞确定罪名的补充规定(四)》。

③ 《最高人民法院、最高人民检察院关于执行＜中华人民共和国刑法＞确定罪名的补充规定(六)》。

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》和《关于办理网络犯罪案件适用刑事诉讼程序若干问题的意见》(公通字 10 号)加以定义。

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。”本罪与“非法侵入计算机信息系统罪”一样，均为 1997 年《刑法》修改时首次加入的涉及危害计算机信息系统犯罪的罪名。

第五，拒不履行信息网络安全管理义务罪。本罪的确立，是明确针对网络服务提供者的信息网络安全管理义务，既可以制裁个人，也可以制裁单位。《刑法》第二百八十六条之一规定：“网络服务提供者不履行法律、行政法规规定的信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，有下列情形之一的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金：（一）致使违法信息大量传播的；（二）致使用户信息泄露，造成严重后果的；（三）致使刑事案件证据灭失，情节严重的；（四）有其他严重情节的”。本罪是 2015 年《刑法修正案（九）》中增设的新罪名。

对于单位作为网络犯罪的入刑，也是针对有组织的网络犯罪活动而新制定的。我国计算机和互联网的发展进入了一个高速发展时期。移动互联网、智能设备以及相关的互联网服务，逐渐替代了传统的以固定终端和软件构成的计算机信息系统应用体系，成为整个社会的主流，中国进入了“互联网＋”时代。在这种时代背景下，网络犯罪行为也发生了巨大的变化，主要表现在以下两个方面。一方面，犯罪主体的类型正在发生变化。过去危害计算机信息系统犯罪的主体多以个人为主，而随着互联网所带来的经济利益的规模不断扩大，受利益的驱使，许多此类犯罪行为都开始朝着集团化的方向发展。因此，犯罪主体已经不再只是个人主体，许多主体是以单位的形式存在。另一方面，网络服务提供者在维护信息安全方面所肩负的责任越来越重要。网络服务提供者本身就有净化网络、合法利用网络的义务，而且它也有保障监管的技术措施。有的网络服务提供者为了提高经营额或经济效益，有意纵容一些利用网络进行违法犯罪的行为，例如网络上出现的各种诈骗、开设赌场、传播淫秽物品等，对社会秩序、人身权利造成了很大威胁。在这种情况下，加强对网络服务提供者有关义务的监督十分必要。

针对这种新的发展趋势，2015 年 8 月 29 日《刑法修正案（九）》针对单位作为网络犯罪主体的新情况做出了补充规定。在《刑法》第二百八十五条中增加一款作为第四款：“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，依照各该款的规定处罚。”在第二百八十六条中增加一款作为第四款：“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。”在第二百八十六条后增加一条，作为第二百八十六条之一，增设“拒不履行信息网络安全管理义务罪”的新罪名。

3.2.2　《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》

1997 年《刑法》和 2009 年出台的《刑法修正案（七）》分别针对危害计算机信息系统安全

的犯罪行为制定了规范并设置了四项具体的罪名，但是在互联网安全威胁日益加剧的情况下，《刑法》中这些相关规范在司法实践中的适用性却不尽如人意。

据公安部的统计数据，近年来，我国互联网上传播的病毒数量平均每年增长80%以上，互联网上平均每10台计算机中有8台受到黑客控制，公安机关受理的黑客攻击破坏活动相关案件平均每年增长110%。而且，通过非法控制计算机信息系统、非法获取计算机信息系统数据、制作销售黑客工具等行为牟取巨额利润，进而逐步形成由制作黑客工具、销售黑客工具、非法获取计算机信息系统数据、控制计算机信息系统、倒卖非法获取的计算机信息系统数据、倒卖非法控制的计算机信息系统的控制权等各个环节构成的利益链条。

因此，严厉打击危害计算机信息系统安全犯罪，加大对信息网络安全的保护力度，对当时的局势而言刻不容缓。然而，在办理危害计算机信息系统案件的过程中，适用《刑法》相关规定遇到了一些问题，需要进一步明确：

（1）《刑法》第二百八十五条、第二百八十六条规定的有关术语，如“专门用于侵入、非法控制计算机信息系统的程序、工具”和“计算机病毒等破坏性程序”等，其含义需做进一步明确。

（2）对犯罪行为的情节和后果缺乏可量化的衡量标准。《刑法》第二百八十五条、第二百八十六条涉及的“情节严重”“情节特别严重”“后果严重”“后果特别严重”等规定缺乏具体认定标准，办案部门认识不一，难以操作。

（3）对于倒卖计算机信息系统数据、控制权等行为的定性、以单位名义或者形式实施危害计算机信息系统安全犯罪的处理、危害计算机信息系统安全共同犯罪的处理等疑难问题，司法实践部门反映突出。

有鉴于此，为适应司法实践需要，明确危害计算机信息系统安全犯罪的法律适用问题，在公安部等有关部门的大力协作下，最高人民法院会同最高人民检察院颁布了《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》（以下简称《危害计算机信息系统安全犯罪解释》）。自2011年9月1日起施行。

《危害计算机信息系统安全犯罪解释》共11个条文，较为全面地明确了危害计算机信息系统安全犯罪涉及的法律适用问题。总体上，可以把《危害计算机信息系统安全犯罪解释》的内容概括为“六个术语界定”“四个定罪量刑标准”和“三个法律适用疑难问题”。

所谓“六个术语界定”，是指：

- “国家事务、国防建设、尖端科学技术领域的计算机信息系统”的界定；
- “计算机信息系统”和“计算机系统”的界定[①]；
- “专门用于侵入、非法控制计算机信息系统的程序、工具”的界定；
- “计算机病毒等破坏性程序”的界定；
- “身份认证信息”的范围界定；

① 这两个术语在《危害计算机信息系统安全犯罪解释》中进行了统一解释，实质是一回事，所以算作一个术语。

- “经济损失”的界定。

这六个术语的具体范围，在危害计算机信息系统安全犯罪司法实践中争论不休，为统一认识，保证相关案件的顺利处理，《危害计算机信息系统安全犯罪解释》对这六个术语作出了统一界定。

所谓“四个定罪量刑标准”，是指：

- 非法获取计算机信息系统数据、控制计算机信息系统行为的定罪量刑标准；
- 提供侵入、非法控制计算机信息系统的程序、工具行为的定罪量刑标准；
- 破坏计算机信息系统功能、数据或者应用程序行为的定罪量刑标准；
- 故意制作、传播计算机病毒等破坏性程序行为的定罪量刑标准。

所谓“三个法律适用疑难问题”，是指：

- 掩饰、隐瞒数据、控制权行为的定性；
- 以单位名义或者形式实施危害计算机信息系统安全犯罪的处理原则[①]；
- 危害计算机信息系统安全共同犯罪的处理原则。

1.《危害计算机信息系统安全犯罪解释》的术语界定

(1) “国家事务、国防建设、尖端科学技术领域的计算机信息系统”的界定。

《危害计算机信息系统安全犯罪解释》第十条规定：对于是否属于刑法第二百八十五条、第二百八十六条规定的“国家事务、国防建设、尖端科学技术领域的计算机信息系统”“专门用于侵入、非法控制计算机信息系统的程序、工具”、“计算机病毒等破坏性程序”难以确定的，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。司法机关根据检验结论，并结合案件具体情况认定。

司法实践一直反映，“国家事务、国防建设、尖端科学技术领域的计算机信息系统”的概念较为模糊，难以系统性地准确把握。例如“尖端科学技术”包括哪些领域的科学技术，难以一一列举，且科学技术发展迅速，当前尖端的科学技术在未来不一定属于尖端科学技术，未来也可能出现新的目前并无法预见到的尖端科学技术。因此，有必要对三大领域的计算机信息系统的范围予以明确。但是，由于各方对这一术语的内涵和外延认识分歧较大，《危害计算机信息系统安全犯罪解释》没有对这一术语作出界定，但是第十条规定，对于是否属于“国家事务、国防建设、尖端科学技术领域的计算机信息系统”难以确定的，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。司法机关根据检验结论，并结合案件具体情况认定。

(2) “计算机信息系统”和“计算机系统”的界定。

《危害计算机信息系统安全犯罪解释》第十一条第一款：“本解释所称‘计算机信息系统’和‘计算机系统’，是指具备自动处理数据功能的系统，包括计算机、网络设备、通信设备、自动化控制设备等。”

---

① 单位犯罪已经在《刑法修正案(九)》中更新，此处失效。

• “计算机信息系统”和“计算机系统”的统一解释。

刑法第二百八十六条关于破坏计算机信息系统罪的规定使用了“计算机信息系统”与“计算机系统”两个概念，其中刑法二百八十六条第三款有关制作、传播计算机病毒等破坏性程序的条款中使用“计算机系统”的概念，其他条款使用“计算机信息系统”的概念。

立法部门和侦查机关统一认为，由于区分这两个概念不存在实质意义，因此对“计算机信息系统”与“计算机系统”两个概念不应作区分，而应进行统一解释。

• “计算机信息系统”和“计算机系统”的界定。

《危害计算机信息系统安全犯罪解释》第十一条第一款规定，“计算机信息系统”和“计算机系统”是指具备自动处理数据功能的系统，包括计算机、网络设备、通信设备、自动化控制设备等。具体而言：

具备自动处理数据功能的设备都可能成为被攻击的对象，有必要将其纳入刑法保护范畴。随着信息技术的发展，各类内置有可以编程、安装程序的操作系统的数字化设备广泛应用于各个领域，其本质与传统的计算机系统已没有任何差别。这些设备都可能受到攻击破坏：互联网上销售的专门用于控制手机的木马程序，可以通过无线网络获取手机中的信息；通过蓝牙、Wi-Fi(将电脑、手持设备等终端以无线方式互相连接的技术)等无线网络传播病毒的案件也呈现快速增长态势；在工业控制设备中可能植入破坏性程序，使得工业控制设备在特定条件下运行不正常；在打印机、传真机等设备中可以内置程序秘密获取相关数据。总之，任何内置有操作系统的智能化设备都可能成为入侵、破坏和传播计算机病毒的对象，因此应当将这些设备的安全纳入刑法保护范畴。

(3)“专门用于侵入、非法控制计算机信息系统的程序、工具”的界定。

① “专门用于侵入、非法控制计算机信息系统的程序、工具”与“专门用于非法获取计算机信息系统数据的程序、工具”的关系。

《刑法》第二百八十五条第三款的用语是“专门用于侵入、非法控制计算机信息系统的程序、工具”，从字面上看，没有涉及专门用于非法获取数据的工具。但是，“所谓‘专门用于侵入计算机系统的程序、工具’，主要是指专门用于非法获取他人登录网络应用服务、计算机系统的账号、密码等认证信息以及智能卡等认证工具的计算机程序、工具。”[①]很显然，除专门用于实施非法侵入计算机信息系统的程序、工具外，通过非法侵入计算机信息系统而非法获取数据的专门性程序、工具也应当纳入“专门用于侵入计算机信息系统的程序、工具”的范畴，这并未超越刑法用语的规范含义。因此，“专门用于侵入、非法控制计算机信息系统的程序、工具”，既包括专门用于侵入、非法控制计算机信息系统的程序、工具，也包括通过侵入计算机信息系统而非法获取数据的专门性程序、工具。顺带需要提及的是，基于同样的理由，刑法第二百八十五条第三款后半句规定的“明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具”，这里的“侵入”既包括非法侵入计算机信息系统行为，

① 黄太云.《刑法修正案(七)》解读.人民检察，2009(6)

也包括通过侵入计算机信息系统而非法获取数据的行为。

具体而言，根据刑法二百八十五条规定的犯罪行为，可以将“专门用于侵入、非法控制计算机信息系统的程序、工具”分为三类：

- 专门用于实施非法侵入计算机信息系统的程序、工具；
- 通过非法侵入计算机信息系统而非法获取数据的专门性程序、工具；
- 专门用于非法控制计算机信息系统的程序、工具。

② “专门用于侵入、非法控制计算机信息系统的程序、工具”与中性程序、工具的界分。

界定“专门用于侵入、非法控制计算机信息系统的程序、工具”，关键在于明确“专门”一词的含义。参考立法机关编写的相关论著，刑法第二百八十五条第三款的“专门用于侵入、非法控制计算机信息系统的程序、工具”，“是指行为人所提供的程序、工具只能用于实施非法侵入、非法控制计算机信息系统的用途。”[①]可见，其区别于一般的程序、工具之处在于此类程序、工具专门是用于违法犯罪目的，而不包括那些既可以用于违法犯罪目的又可以用于合法目的的“中性程序”。因此，“专门”是对程序、工具本身的用途非法性的限定，是通过程序、工具本身的用途予以体现的。而程序、工具本身的用途又是由其功能所决定的，如果某款程序、工具在功能设计上就只能用来实施控制、获取数据的违法行为，则可以称之为“专门工具、程序”。经研究认为，从功能设计上可以对“专门用于侵入、非法控制计算机信息系统的程序、工具”作如下限定：

首先，程序、工具本身具有获取计算机信息系统数据、控制计算机信息系统的功能。如前所述，从刑法规范的逻辑角度而言，刑法第二百八十五条第三款应当是前两款的工具犯。刑法第二百八十五条第三款规定的“专门用于侵入、非法控制计算机信息系统的程序、工具”实质上是指专门用于实施刑法二百八十五条规定之罪的程序、工具。需要注意的是，由于专门用于实施非法侵入计算机信息系统的程序、工具较为少见，而且难以从功能上对其做出界定，对其主要应通过主观设计目的予以判断（即《危害计算机信息系统安全犯罪解释》第二条第（三）项的规定）。基于上述考虑，这里主要强调了程序、工具本身的获取数据和控制功能。

其次，程序、工具本身具有避开或者突破计算机信息系统安全保护措施的功能。有不少木马程序既可用于合法目的，也可用于非法目的，属于“中性程序”，比如系统自带的 Terminal Service（终端服务），也可以用于远程控制计算机信息系统，很多商用用户运用这种远程控制程序以远程维护计算机信息系统。通常情况下，攻击者使用的木马程序必须故意逃避杀毒程序的查杀和防火墙的控制，故此类木马程序区别于“中性的”商用远程控制程序的主要特征是其具有“避开或者突破计算机信息系统安全保护措施”的特征，如自动停止杀毒软件的功能、自动卸载杀毒软件功能等，在互联网上广泛销售的所谓“免杀”木马程序即属于此种类型的木马程序。因此，《危害计算机信息系统安全犯罪解释》将“专门用于避开或

① 全国人大常委会法工委刑法室. 中华人民共和国刑法·条文说明、立法理由及相关规定. 北京：北京大学出版社，2009：592

者突破计算机信息系统安全保护措施”作为界定标准之一。

最后，程序、工具获取数据和控制的功能在设计上即能在未经授权或者超越授权的状态下得以实现。这是专门程序、工具区别于“中性程序、工具”的典型特征，是该类程序违法性的集中体现。例如“网银大盗”程序，其通过键盘记录的方式，监视用户操作，当用户使用个人网上银行进行交易时，该程序会恶意记录用户所使用的账号和密码，记录成功后，程序会将盗取的账号和密码发送给行为人。该程序在功能设计上即可在无须权利人授权的情况下获取其网上银行账号、密码等数据。“中性”程序、工具不具备在未经授权或超越授权的情况下自动获取数据或者控制他人计算机信息系统的功能。

(4)“计算机病毒等破坏性程序”的界定。

刑法第二百八十六条第三款将故意制作、传播计算机病毒等破坏性程序的行为规定为犯罪。因此，准确界定“计算机病毒等破坏性程序”的范围，对于处理相关案件至关重要。《危害计算机信息系统安全犯罪解释》第五条对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”的范围进行了明确。

• “计算机病毒等破坏性程序”的具体范围。

基于上述考虑，《危害计算机信息系统安全犯罪解释》第五条对“计算机病毒等破坏性程序”的具体范围作了规定。具体包括：

计算机病毒，即能够通过网络、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程序。计算机病毒的危害性主要是其传播方式容易引起大规模传播，而且一经传播即无法控制其传播面，也无法对被侵害的计算机逐一取证并确认其危害后果。换言之，计算机病毒的传播必然会影响计算机系统的正常运行，属于破坏性程序的范畴。

逻辑炸弹，即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程序。此类程序一旦被触发即可破坏计算机信息系统数据、功能或者应用程序，但在未触发之前仍存在潜在的破坏性。同样，此种程序应当纳入破坏性程序的范畴。

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。

• “计算机病毒等破坏性程序”的认定程序。

同“专门用于侵入、非法控制计算机信息系统的程序、工具”的认定一样，根据《危害计算机信息系统安全犯罪解释》第十条的规定，对于“计算机病毒等破坏性程序”难以确定的，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。司法机关根据检验结论，结合侵入行为、侵入方法、侵入后果等相关情况认定。此外，根据《网络犯罪刑事诉讼程序意见》的规定，对电子数据涉及的专门性问题难以确定的，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检验报告。据此，对于是否属于计算机病毒等破坏性程序，也可以由公安部指定的机构出具检验报告。

(5)“身份认证信息”的界定。

《危害计算机信息系统安全犯罪解释》第十一条第二款规定：“本解释所称‘身份认证信

息’，是指用于确认用户在计算机信息系统上操作权限的数据，包括账号、口令、密码、数字证书等。”

由于《危害计算机信息系统安全犯罪解释》多处涉及“身份认证信息”这一术语，第十一条第二款明确了“身份认证信息”的内涵和外延。考虑到司法实践的具体情形，采用了概括加列举的方法，将“身份认证信息”界定为用于确认用户在计算机信息系统上操作权限的数据，包括账号、口令、密码、数字证书等。从实践来看，数字签名、生物特征等都属于身份认证信息。

(6)“经济损失”的界定。

《危害计算机信息系统安全犯罪解释》第十一条第三款规定：“本解释所称‘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。”

根据《危害计算机信息系统安全犯罪解释》的规定，危害计算机信息系统安全犯罪以造成经济损失的数额作为入罪标准之一。为统一法律适用，《危害计算机信息系统安全犯罪解释》第十一条第三款明确了“经济损失”的计算范围，具体包括危害计算机信息系统犯罪行为给用户造成的直接经济损失，以及用户为恢复数据、功能而支出的必要费用。需要注意的是，破坏计算机信息系统功能、数据给用户带来的预期利益的损失不能纳入“经济损失”的计算范围。具体而言包括：

① 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。

对于非法获取计算机信息系统数据犯罪而言，合法用户获取该数据应当支付的费用属于该行为给用户直接造成的经济损失。例如，付费后才能查阅小说的文学网站，如果非法获取该网站中的小说，则查阅这些小说的合法用户应当支付的费用属于该网站运营者的经济损失；如果不需要付费则可以获得的数据，则未造成损失；如果不管付费不付费都不对外提供的数据，则难以衡量经济损失，例如侵入他人计算机并获取该用户的私人照片，则无法衡量经济损失，只能按照其他量刑标准处理。

对于通过非法控制计算机信息系统使用的计算机信息系统资源，合法用户使用该计算机信息系统资源应当支付的费用属于行为给用户直接造成的经济损失。例如，侵入某个托管主机并使用该托管主机的虚拟空间，则其少支付的费用则属于托管主机运营商的经济损失。对于并未提供付费服务的计算机信息系统，由于属于使用盗窃范畴，则难以衡量其经济损失，只能按照其他量刑标准处理。

计算机信息系统不能正常运行期间支付的网络带宽费用等合理支出费用。对于造成计算机信息系统功能无法正常运行，比如对某个网站实施拒绝服务攻击，则该网站的所有者在被拒绝服务攻击期间支付的主机托管、系统维护等费用都属于造成的损失。

② 用户为恢复数据、功能而支出的必要费用。

在计算机信息系统功能或者数据被破坏后，通常需要采取各种应急响应措施使其恢复到正常状态，如对于被删除的数据采取数据恢复措施，被拒绝服务攻击的网站增加数据分流

设备、增加带宽等，这都属于造成的经济损失。

③ 用户预期利益的损失不纳入“经济损失”的计算范围。

越来越多的经济活动对计算机信息系统的依赖程度很强，如果破坏计算机信息系统的数据或者功能可能造成重大的收入损失，但如果该损失属于预期利益的损失，如丧失商业合作机会造成的经济损失，则不能纳入“经济损失”的计算范围。

2.《危害计算机信息系统安全犯罪解释》定罪量刑标准

(1) 非法获取计算机信息系统数据、控制计算机信息系统罪的定罪量刑标准。

① 定罪量刑标准设定的背景。

《刑法修正案(七)》将非法获取计算机信息系统数据行为入罪，主要是为了解决网络盗窃计算机信息系统数据的法律适用问题。具体而言：

对于非法获取法律属性尚未明确的计算机信息系统数据的行为，存在法律适用困难。当前，在计算机信息系统中存储、处理或者传输的数据，因其包含内容的不同而具有不同的法律属性。其中，有些计算机信息系统数据的法律属性明确，如非法获取涉及国家秘密、商业秘密的计算机信息系统数据的，可以依照非法获取国家秘密罪、侵犯商业秘密罪等犯罪论处。但是，也存在着一些法律属性尚未明确的计算机信息系统数据，如作为当前网络盗窃主要对象的网络账号、网络游戏装备等“虚拟财产”。由于“虚拟财产”的财产属性存在争议，能否认定为公私财产存在不同意见；而且，即使认定为公私财产，由于发行数量与价格指数完全由网络运营商控制，与现实社会的物价指数无必然联系，难以制定出科学合理的价格认定的方法。因此，对于非法获取“虚拟财产”等计算机信息系统数据的行为，难以适用传统的盗窃罪。

对计算机信息系统数据“使用盗窃”的行为，难以适用盗窃罪准确定罪量刑。不少情况下，非法获取计算机信息系统数据行为所获得的只是数据的使用权，而不是数据的所有权。如非法获得拨号上网账号并使用该账号免费上网，实质上盗窃者获得的是账号的使用权而不是所有权。在合法用户包月使用的情况下，难以确定行为人究竟应当支付多少费用，也就难以衡量造成的经济损失或者获利情况。

对于非法获取计算机信息系统数据，但是尚未实际使用该数据，无法适用盗窃罪等传统罪名。例如，非法获取网上银行账号、密码，但是尚未使用该账号、密码和转移其中的资金，无法按照盗窃罪定罪处罚。基于上述原因，《刑法修正案(七)》将非法获取计算机信息系统数据行为单独入罪，规定为专门的非法获取计算机信息系统数据罪，以区别于传统的盗窃罪等犯罪。

② 定罪量刑标准设定的适用范围。

根据《刑法》第二百八十五条第二款的规定，违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据的，构成非法获取计算机信息系统数据罪。因此，该罪所保护的主要是计算机信息系统安全。对于非法获取计算机信息系统数据进而实施其他犯罪的行为，可以依照其他犯罪处理，如非法获取网上银行账号、密码后转移账户资

金的，可以按照盗窃罪定罪处罚。行为人非法获取网上银行账号、密码但并未窃取账户资金的行为，由于侵犯了计算机信息系统安全，如果情节严重，也应当按照非法获取计算机信息系统罪定罪处罚。

基于上述分析，《危害计算机信息系统安全犯罪解释》第一条在设定非法获取计算机信息系统数据、控制计算机信息系统罪定罪量刑标准时主要有如下考虑：

a. 非法获取数据罪主要并不以数据自身的法律属性来衡量其犯罪情节，而应当主要以其对计算机信息系统的安全造成的危害程度来衡量其犯罪情节。

b. 非法获取计算机信息系统数据罪应当解决的问题主要是数据的法律属性不明确，无法适用刑法其他条款的情形。例如获取的国家秘密、商业秘密等法律属性明确的数据的，可以依照其他罪种定罪处罚，非法获取数据罪主要是应当对非法获取数据行为定罪处罚而又无法按照刑法其他条款定罪处罚的情形提供法律依据。

c. 无论是非法获取计算机信息数据，还是非法控制计算机信息系统，主要动机都是牟利，故应当将以牟利为目的的非法获取数据的行为作为重点打击对象。

③ 入罪标准。

• 获取网络金融服务的身份认证信息构成“情节严重”的情形。

与计算机信息系统安全相关的数据中最为重要的是用于认证用户身份的身份认证信息（如口令、证书等），此类数据通常是网络安全的第一道防线，也是网络盗窃的最主要对象。特别是非法获取电子银行、证券交易、期货交易等网络金融服务的账号、口令等身份认证信息的活动非常猖獗。从实践来看，不少行为人在非法获取相关账号、密码后并不转移该账号中的资金，而是将账号、密码等数据销售给他人获利。基于此，《危害计算机信息系统安全犯罪解释》对网络金融服务的身份认证信息予以重点保护，根据司法实践的情况，综合行为的社会危害性，规定“获取支付结算、证券交易、期货交易等网络金融服务的身份认证信息十组以上的”构成非法获取计算机信息系统数据“情节严重”。

立法机关经研究认为，非法获取网络金融服务的身份认证信息的行为与伪造信用卡的行为存在一定的差异，前者可能并不能直接窃取账户资金（如在账户所有人修改密码的情况下），而后者可以直接窃取资金。基于此，两者在入罪标准方面应当有所差异。因此，综合考虑司法实践的情况，《危害计算机信息系统安全犯罪解释》将非法获取网络金融服务的身份认证信息的入罪标准设定为“十组以上”。

• 获取其他身份认证信息构成“情节严重”的情形。

对于网络金融服务的身份认证信息以外的其他网络服务的身份认证信息，如网络即时通讯、网络邮箱等的身份认证信息，网络盗窃者非法获取这些身份认证信息的案件也较为多发。实践中，网络盗窃者非法获取上述身份认证信息，通常有三种目的：一是通过销售这些账号信息或者窃取这些账号中的虚拟财产（如游戏装备、Q 币等）获利；二是通过使用这些账号信息减少自己的费用支出，如盗窃他人拨号上网账号上网以减少支付费用；三是通过使用这些账号实施其他违法犯罪行为，如窃取 QQ 号码后骗取 QQ 好友的钱财，盗窃邮箱账

号后查看他人邮箱内容等。根据司法实践中的具体情况,《危害计算机信息系统安全犯罪解释》规定获取网络金融服务以外的身份认证信息“五百组以上的”构成非法获取计算机信息系统数据“情节严重”。

司法实践中,要准确把握《危害计算机信息系统安全犯罪解释》规定的一“组”身份认证信息的概念。所谓一组身份认证信息,是指可以确认用户在计算机信息系统上操作权限的认证信息的一个组合,例如某些网上银行需要用户名、密码和动态口令就可以转账,那么用户名、密码和动态口令就是一组身份认证信息;有的网上银行除上述三项信息外还需要手机认证码才可以转账,缺一不可,那么这四项信息才能构成一组身份认证信息。但是,对于身份认证信息,特别是密码信息,很多用户有经常更改密码的习惯,故认定一组身份认证信息不应以在办案过程中是否可以实际登录使用为判断标准,而应结合其非法获取身份认证信息的方法判断该身份认证信息在被非法获取时是否可用为依据,如使用的木马程序能有效截获用户输入的账号密码,则不管该密码当前是否可用,只要是使用该木马程序截获的账号、密码,则应认定为一组有效身份认证信息。

• 非法控制计算机信息系统构成“情节严重”的情形。

在非法侵入计算机信息系统后,并未破坏计算机信息系统的功能或者数据,而是通过控制计算机信息系统实施特定操作的行为被称为“非法控制计算机信息系统”。很多攻击者通过控制大量计算机信息系统形成僵尸网络(BOTNET),据统计,全世界的僵尸网络 75%位于我国,有的僵尸网络控制的计算机信息系统甚至多达数十万台,这已成为我国互联网安全的重大隐患。针对上述问题,《危害计算机信息系统安全犯罪解释》将非法控制计算机信息系统台数作为衡量情节严重的标准之一,即非法控制计算机信息系统二十台以上的,应当认定为“情节严重”。

• 违法所得或者造成经济损失构成“情节严重”的情形。

非法获取计算机信息系统数据、控制计算机信息系统行为的主要目的是牟利,且易给权利人造成经济损失,因此,《危害计算机信息系统安全犯罪解释》将违法所得数额和财产损失数额作为衡量情节严重的标准之一。

从实践来看,难以对身份认证信息以外的计算机信息系统数据的入罪标准作出统一规定。例如,入侵教育部门证件信息查询系统并获取毕业证、学位证信息的行为,具体的入罪标准就难以设定。此外,有些非法获取身份认证信息、非法控制计算机信息系统的行为,虽然数量未达到前述标准,但非法获利数额可能非常大,如盗窃一个 QQ 号码销售获利数万元,有必要予以刑事惩治。基于上述考虑,《危害计算机信息系统安全犯罪解释》将违法所得作为入罪标准之一,规定违法所得五千元以上的构成“情节严重”。

非法获取计算机信息系统数据和非法控制计算机信息系统可能造成经济损失,如获取他人拨号上网账号后使用该账号免费上网,可能给网络接入服务商造成经济损失;获取网上需要付费的服务(如网上查询高考成绩通常需要付费)的账号并使用该账号获得服务并规避支付费用,实质上给服务提供商造成了收入上的损失;非法控制计算机信息系统如控制

托管服务商的主机并免费使用主机上的存储空间建设网站，实际上造成了托管服务商的主机出租收入的损失。基于此，《危害计算机信息系统安全犯罪解释》将造成经济损失作为入罪标准之一，规定造成经济损失一万元以上的构成“情节严重”。

• 其他构成“情节严重”的情形。

考虑到司法实践的情况十分复杂，《危害计算机信息系统安全犯罪解释》设置了兜底项，对于不符合上述情形，但确实达到情节严重程度，如造成恶劣社会影响的，也可以按照犯罪处理。

(2) 提供侵入、非法控制计算机信息系统的程序、工具罪的定罪量刑标准。

《刑法》第二百八十五条第三款规定了提供侵入、非法控制计算机信息系统的程序、工具罪，具体包括提供专门用于侵入、非法控制计算机信息系统的程序、工具和明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具两种行为方式。因此，明确“专门用于侵入、非法控制计算机信息系统的程序、工具”的范围，对于处理相关案件具有重要意义。《危害计算机信息系统安全犯罪解释》第二条对《刑法》第二百八十五条第三款规定的“专门用于侵入、非法控制计算机信息系统的程序、工具”的范围进行了明确。

① “专门用于侵入、非法控制计算机信息系统的程序、工具”的认定程序。

专门用于侵入、非法控制计算机信息系统的程序、工具由于专业性较强，根据《危害计算机信息系统安全犯罪解释》第十条的规定，应当委托省级以上负责计算机信息系统安全管理工作的部门检验，司法机关根据检验结论，并结合案件具体情况认定。关于检验部门的具体范围，应当根据《计算机信息系统安全保护条例》(国务院第 147 号令)第六条的规定确定。该条规定：“公安部主管全国计算机信息系统安全保护工作。国家安全部、国家保密局和国务院其他有关部门，在国务院规定的职责范围内做好计算机信息系统安全保护的有关工作。”因此，在司法实践中，应当根据案件的具体情况，由公安机关、安全机构或者保密部门等出具检验结论。必要时，为了确保司法认定的准确性，也可以委托具有相关鉴定资质的司法鉴定机构进行鉴定，检验部门结合鉴定意见综合判断后出具检验意见。最终，司法机关根据检验结论，并结合案件具体情况认定。

② 定罪量刑标准。

• 提供侵入、非法控制计算机信息系统程序、工具罪定罪量刑标准。

第三条第一款明确了“情节严重”的具体认定标准。对于提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具的行为，主要从以下几个方面认定“情节严重”：

一是提供的程序、工具的人次。其中，对于提供网银木马等“能够用于非法获取支付结算、证券交易、期货交易等网络金融服务的身份认证信息的专门性程序、工具”的行为，第(一)项规定提供五人次以上的即属“情节严重”；对于提供盗号程序、远程控制木马程序等其他专门用于侵入、非法控制计算机信息系统的程序、工具的，第(二)项规定提供的人次达到二十人次以上的属于“情节严重”；对于明知他人实施非法获取支付结算、证券交易、期货

交易等网络金融服务的身份认证信息的违法犯罪行为而为其提供程序、工具的，第（三）项规定提供五人次以上的即属“情节严重”；对于明知他人实施其他侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具的，第（四）项规定提供二十人次以上的属于“情节严重”。

二是违法所得和经济损失数额。由于提供此类工具的行为主要以获利为目的，正是在非法获利的驱动下，互联网上销售各类黑客工具的行为才会泛滥，且往往会给权利人造成经济损失，故第（五）项将违法所得五千元以上或者造成经济损失一万元以上作为认定“情节严重”的标准之一。

三是对于其他无法按照提供的人次、违法所得数额、经济损失数额定罪的，第（六）项设置了兜底条款。

此外，第二款规定“情节严重”和“情节特别严重”之间为五倍的倍数关系。

• 提供侵入、非法控制计算机信息系统程序、工具犯罪案件办理中应当注意的问题。

《刑法》第二百八十五条第三款实际上是《刑法》第二百八十五条第一款、第二款的工具犯。该款规定，提供专门用于侵入（包括通过侵入计算机信息系统实施的非法获取数据）、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入（包括通过侵入计算机信息系统实施的非法获取数据）、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，情节严重的，以提供侵入、非法控制计算机信息系统的程序、工具罪论处。在司法实践中，要注意把握刑法第二百八十五条第一款、第二款与第三款相交织的情形：

一是明知他人实施侵入（包括通过侵入计算机信息系统实施的非法获取数据）、非法控制计算机信息系统的违法犯罪行为，而为其提供程序、工具行为的定性。从立法背景来看，《刑法修正案（七）》增设了刑法第二百八十五条第三款，将非法侵入计算机信息系统、非法获取计算机信息系统数据、控制计算机信息系统共同犯罪中的提供工具行为独立化，单独规定为犯罪，并配置了独立的法定刑。在此背景下，对于明知他人实施侵入（包括通过侵入计算机信息系统实施的非法获取数据）、非法控制计算机信息系统的违法犯罪行为，而为其提供程序、工具的，无论是否构成共同犯罪，均应以提供侵入、非法控制计算机信息系统的程序、工具罪论处。

二是明知他人实施侵入（包括通过侵入计算机信息系统实施的非法获取数据）、非法控制计算机信息系统的违法犯罪行为，而为其提供程序、工具，并参与实施了非法侵入计算机信息系统、非法获取计算机信息系统数据、控制计算机信息系统的具体犯罪行为的定性。本书认为，行为人实施的行为既符合了非法侵入计算机信息系统罪或者非法获取计算机信息系统数据、控制计算机信息系统罪，也符合了提供侵入、非法控制计算机信息系统的程序、工具罪，但是考虑到两个行为之间前后相连，密不可分，不宜再数罪并罚。较为妥善的处理方案是，按照“从一重处断”原则，比较两罪轻重，按照重罪处断。

（3）破坏计算机信息系统罪的定罪量刑标准。

① 定罪量刑标准设定的主要考虑。

• 数据、应用程序均可以成为破坏计算机信息系统行为的对象。

《刑法》第二百八十六条第二款规定："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，依照前款的规定处理。"需要注意的是，关于"数据和应用程序"之间究竟是择一关系还是并列关系，即破坏计算机信息系统数据或者应用程序，就可构成破坏计算机信息系统罪，还是只有同时破坏计算机信息系统数据和应用程序，才能构成破坏计算机信息系统罪，存有不同认识。本书认为，基于司法实践的具体情况，从体系解释的角度，应当将其理解为择一关系，即刑法第二百八十六条第二款规定的"数据和应用程序"应当理解为数据、应用程序均可以成为犯罪对象。主要考虑如下：

第一，从司法实践来看，破坏数据、应用程序的案件，主要表现为对数据进删除、修改、增加的操作，鲜有破坏应用程序的案件。因此，对于《刑法》第二百八十六条"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"的规定，应当理解为数据、应用程序均可以成为犯罪对象，并不要求一次破坏行为必须同时破坏数据和应用程序，这样才能实现对计算机信息系统中存储、处理或者传输的数据、应用程序的有效保护，维护计算机信息系统安全。

第二，上述认识在以往的司法解释中有先例可循。《走私犯罪解释》第四条就将刑法第一百五十一条第二款规定的"珍贵动物及其制品"解释为"珍贵动物或者其制品"。因此，数据、应用程序均可以成为破坏计算机信息系统罪的对象，并不要求一次破坏行为必须同时破坏数据和应用程序。基于这一认识，《危害计算机信息系统安全犯罪解释》第四条第一款第(二)项规定，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，即构成破坏计算机信息系统罪。需要注意的是，由于以计算机信息系统应用程序为破坏对象的案件很少，这里并未规定以被破坏应用程序的计算机信息系统的台数为定罪量刑标准，而主要是通过违法所得和造成经济损失的数额定罪量刑。

• 破坏计算机信息系统数据、应用程序的把握。

根据《刑法》第二百八十六条第二款的规定，破坏计算机信息系统数据、应用程序行为有删除、修改、增加三种方式。所谓"删除"，是指将计算机信息系统中存储、处理或者传输的数据、应用程序删去，既可以是全部删除，也可以是部分删除。所谓"修改"，是指对计算机信息系统数据、应用程序进行改动。所谓"增加"，是指在计算机信息系统中增加新的数据、应用程序。需要注意的是，对计算机信息系统数据、应用程序删除、修改、增加的三种操作方式，即通常所讲的对数据、应用程序的"增删改"，在社会危害性上没有什么区别，都是破坏数据、应用程序，这一点在司法实践中应注意把握。

破坏计算机信息系统数据、应用程序入罪不以被破坏的数据无法恢复为要件。根据《刑法》第二百八十六条第二款的规定，只要对计算机信息系统数据进行删除、修改、增加的操作即可，至于被破坏的数据是否可以恢复到破坏前的状态，并非入罪要件。而且，将被破坏的数据是否可以恢复作为入罪条件，也不具有可操作性。被破坏的数据，一般技术人员无法恢

复的，可能技术专家就能恢复，故被破坏的数据是否可以恢复是一个无从判断的标准。此外，与其他两种破坏计算机信息系统的行为方式不同，破坏计算机信息系统数据和应用程序构成破坏计算机信息系统罪，并不要求达到“造成计算机信息系统不能正常运行”或者“影响计算机系统正常运行”的结果。换言之，破坏计算机信息系统数据、应用程序的情形，在入罪要件方面不同于其他两类破坏计算机信息系统的情形。

• 针对特定类型或者特定领域的计算机信息系统的特殊保护。

在网络上存在很多为其他计算机信息系统提供基础服务的系统，如域名解析服务器、路由器、身份认证服务器、计费服务器等，对这些服务器实施攻击可能导致大量的计算机信息系统瘫痪，例如一个域名解析服务器可能为数万个网站提供域名解析服务，对其实施拒绝服务攻击将可能导致数万个网站无法访问，表面上其攻击行为仅破坏了一台服务器的功能，但由此引发的后果却远大于此。此外，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承担着公共服务职能，对其的攻击破坏后果更为严重，社会危害性更大。因此，针对特定类型或者特定领域计算机信息系统的攻击是互联网上危害最为严重的攻击行为，应当对其作出专门规定。

《危害计算机信息系统安全犯罪解释》起草过程中，曾将针对特定类型或者特定领域的计算机信息系统破坏活动规定为破坏计算机信息系统罪的从重处罚情节。经研究认为，为了体现对特定领域计算机信息系统的特殊保护，应当设定单独的定罪量刑标准。因此，《危害计算机信息系统安全犯罪解释》将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情形直接规定为“后果特别严重”。

② 入罪标准。

《危害计算机信息系统安全犯罪解释》第四条第一款规定了“后果严重”的具体认定标准。对于破坏计算机信息系统功能、数据或者应用程序行为，主要从以下几个方面认定“后果严重”：

破坏计算机信息系统的数量。

第一，《危害计算机信息系统安全犯罪解释》规定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，属于“后果严重”。需要注意的是，“计算机信息系统的主要软件或者硬件不能正常运行”，不能仅仅理解为计算机信息系统不能启动或者不能进入操作系统等极端情况，而是既包括计算机信息系统主要软件或者硬件的全部功能不能正常运行，也包括计算机信息系统主要软件或者硬件的部分功能不能正常运行。

第二，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、增加的操作的，应当认定为“后果严重”。

违法所得、经济损失的数额。从司法实践来看，存在通过破坏计算机信息系统功能、数据或者应用程序直接获利或者间接获利的情形。例如对于拒绝服务攻击，有的收取他人费用并帮助他人实施拒绝服务攻击，也有的通过拒绝服务攻击他人网站后向被攻击的网站的

管理者推销防火墙等产品获利，这两种情况分别属于直接获利或者间接获利。基于此，《危害计算机信息系统安全犯罪解释》规定违法所得五千元以上或者造成经济损失一万元以上的属于“后果严重”。

在《危害计算机信息系统安全犯罪解释》起草过程中，关于“违法所得数额”能否作为确定“后果严重”和“后果特别严重”的标准问题，有意见提出了质疑。经慎重研究，认为：“违法所得数额”是目前司法实践中最好操作的标准，而且违法所得越多，通常也会给权利人带来相应严重的后果，故具有相对合理性。因此，对“违法所得数额”予以保留。

针对特定类型的计算机信息系统作出特殊规定。《危害计算机信息系统安全犯罪解释》规定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，属于“后果严重”。司法实务中应当注意的是，认定被破坏的计算机信息系统是否属于本款第（四）项中的“为一万以上用户提供服务的计算机信息系统”和第二款第（二）项中“为五万以上用户提供服务的计算机信息系统”，可采用如下方法：有注册用户的按照其注册用户数量统计，没有注册用户的按照其服务对象的数量统计。此外，第（五）项为兜底条款。

《危害计算机信息系统安全犯罪解释》第四条第二款规定了“后果特别严重”的具体情形。第（一）项规定，通常情况下，“后果严重”和“后果特别严重”之间为五倍的倍数关系。第（二）项针对为其他计算机信息系统提供基础服务或者其他服务的特定类型计算机信息系统作出特殊规定。此外，国家机关或者金融、电信、交通、教育、医疗、能源领域的计算机信息系统主要用于提供公共服务。考虑到此类计算机信息系统的特殊性，第（三）项将破坏该类计算机信息系统的功能或者数据，致使生产、生活受到严重影响或者造成恶劣社会影响的情形规定为“后果特别严重”。

（4）故意制作、传播计算机病毒等破坏性程序行为的定罪量刑标准。

根据《刑法》第二百八十六条第三款的规定，故意制作、传播计算机病毒等破坏性程序行为设有两个法定刑档次：后果严重的，符合基本法定刑档次，处五年以下有期徒刑或者拘役；后果特别严重的，构成结果加重犯，处五年以上有期徒刑。为统一司法适用，《危害计算机信息系统安全犯罪解释》第六条对故意制作、传播计算机病毒等破坏性程序“后果严重”和“后果特别严重”的具体情形作了规定，明确了定罪量刑标准。

① 起草背景。

根据《刑法》第二百八十六条第三款的规定，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，是破坏计算机信息系统的一种情形。《危害计算机信息系统安全犯罪解释》起草过程中，着重考虑了如下两个问题：

• 故意制作、传播计算机病毒行为并非独立的提供工具犯。

《刑法》第二百八十六条第三款对制作、传播计算机病毒等破坏性程序作出了规定，但这一规定有别于《刑法》第二百八十五条第三款关于提供侵入、非法控制计算机信息系统的程序、工具罪的规定，后者是独立的提供工具犯，对于提供侵入、非法控制计算机信息系统的程

序、工具的行为可予以独立打击，而前者并非独立的工具犯罪，制作、销售计算机病毒等破坏性程序的行为是否构成犯罪取决于其是否“影响计算机系统正常运行”。故意制作、传播计算机病毒等破坏性程序是破坏计算机信息系统罪的一种行为方式，故意制作计算机病毒并销售，但病毒并未被植入计算机信息系统，不可能给计算机信息系统造成影响，不能依照破坏计算机信息系统罪定罪处罚。因此，对于互联网上制作、销售计算机病毒等破坏性程序的行为无法像制作、提供专门用于非法控制计算机信息系统、非法获取数据的程序的行为那样进行独立打击，只有制作、提供的计算机病毒等破坏性程序最终被使用并产生影响计算机信息系统正常运行后果的行为，才能依据破坏计算机信息系统罪予以打击。例如，备受社会各界关注的“熊猫烧香”病毒案。2006 年 10 月，行为人李×编写了“熊猫烧香”病毒并在网上广泛传播，并且还以自己出售和由他人代卖的方式，在网络上将该病毒销售给 120 余人，非法获利 10 万余元。经病毒购买者进一步传播，导致该病毒的各种变种在网上大面积传播，对互联网用户计算机安全造成了严重破坏。李×还于 2003 年编写了“武汉男生”病毒，于 2005 年编写了“武汉男生 2005”病毒及“QQ 尾巴”病毒。此外，其他行为人通过改写、传播“熊猫烧香”等病毒，构建“僵尸网络”，通过盗窃各种游戏和 QQ 账号等方式非法牟利。法院认定被告人李×犯破坏计算机信息系统罪，判处有期徒刑四年；其他被告人也构成破坏计算机信息系统罪，判处相应刑罚。本案中，行为人李×等制作、传播“熊猫烧香”等病毒，若未造成影响计算机信息系统正常运行的后果，尚不构成破坏计算机信息系统罪。但在本案中，被告人李×等制作、传播的计算机病毒，特别是“熊猫烧香”病毒及其变种在互联网上通过多种方式大规模传播，并将感染的所有程序文件改成熊猫举着三根香的模样，同时该病毒还具有盗取用户游戏账号、QQ 账号等功能。该病毒传播速度快，危害范围广，有上百万个人用户、网吧及企业局域网用户遭受感染和破坏，严重影响了众多计算机系统正常运行，后果严重，应当认定为破坏计算机信息系统罪。

• 将一对一提供计算机病毒等破坏性程序的情形纳入刑事规制范围。

基于危害计算机信息系统安全犯罪的特殊性，宜将一对一的情形也理解为“传播”，即针对某个计算机实施病毒破坏的行为，也应视为“故意传播计算机病毒等破坏性程序”。但是上述行为必须最终导致“影响计算机信息系统正常运行”，即其制作、提供的计算机病毒等破坏性程序最终被使用并产生后果，否则不能认定为破坏计算机信息系统罪。

② 定罪量刑标准。

《危害计算机信息系统安全犯罪解释》第六条第一款明确了故意制作、传播计算机病毒等破坏性程序“后果严重”的具体认定标准。该司法解释第五条第(一)项规定了计算机病毒程序具有自我复制传播特性，其传播方式容易引起大规模传播。由于此类程序一经传播即无法控制其传播面，也无法对被侵害的计算机逐一取证确认其危害后果，因此，《危害计算机信息系统安全犯罪解释》规定制作、提供、传输该类程序，只要导致该程序通过网络、存储介质、文件等媒介传播的，即应当认定为“后果严重”。而“逻辑炸弹”等其他破坏性程序在未触发之前，并不破坏计算机信息系统，只存在潜在的破坏性，只有向被害计算机信息系统植入

该程序，才满足“影响计算机信息系统正常运行”的要件。因此，《危害计算机信息系统安全犯罪解释》规定向二十台以上计算机系统植入其他的破坏性程序的，应当认定为“后果严重”。以提供计算机病毒等破坏性程序的人次、违法所得数额、经济损失数额作为衡量“后果严重”的标准，《危害计算机信息系统安全犯罪解释》规定提供计算机病毒等破坏性程序十人次以上、违法所得五千元以上或者造成经济损失一万元以上属于后果严重。此外，第六条还设置了兜底条款。

第六条第二款规定了“后果特别严重”的认定标准。计算机病毒容易被大规模传播，且一经传播即无法控制其传播面，故第(一)项特别规定制作、提供、传输计算机病毒，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，应属“后果特别严重”。其他情况下，“后果严重”和“后果特别严重”之间为五倍的倍数关系。

3.《危害计算机信息系统安全犯罪解释》法律适用疑难问题

(1) 掩饰、隐瞒计算机信息系统数据、控制权行为的定性。

危害计算机信息系统安全犯罪活动的一个重要特点是分工细化。例如，在非法获取计算机信息系统数据活动中，制作非法获取数据的程序、传播用于非法获取数据的程序、非法获取数据、获取数据后销赃获利、使用数据等行为通常由不同人员实施。这些行为由于行为人之间事前无通谋，欠缺共同犯罪故意，难以依据共同犯罪予以打击。目前，收购、代为销售或者以其他方法掩饰、隐瞒计算机信息系统数据、控制权的行为已经非常泛滥，甚至形成了大规模的网上交易平台。

《危害计算机信息系统安全犯罪解释》第七条明确了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、隐瞒行为的定性问题。

《危害计算机信息系统安全犯罪解释》起草过程中，最初拟将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，而予以倒卖的行为以非法获取计算机信息系统数据、控制计算机信息系统罪的共同犯罪论处。经深入研究，未采纳上述方案。主要考虑如下：其一，倒卖非法获取的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的行为，在危害计算机信息系统安全犯罪中起到了重要的作用，实际危害十分严重。如果将其作为共同犯罪处理，假如非法获取计算机信息系统数据、控制计算机信息系统的行为人未达到入罪的标准，则无法将倒卖者作为共犯处理。其二，计算机信息系统数据、控制权的倒卖通常环节众多，规模庞大，要查清每个计算机信息系统数据、控制权的具体来源几乎不可能，如果按照共同犯罪处理，则获利最大的倒卖者容易逃避打击。

《刑法修正案(六)》《刑法修正案(七)》均对 1997 年刑法第三百一十二条进行了修改，形成了现在的表述。从现行规定来看，《刑法》第三百一十二条的对象不限于赃物，而是涵盖除《刑法》第一百九十一条规定的洗钱罪的上游犯罪以外的所有犯罪的犯罪所得及其产生的收

益。因此，“刑法第三百一十二条的适用范围就扩大到了除刑法第一百九十一条规定的上游犯罪以外的所有犯罪。”[①]基于上述考虑，刑法第二百八十五条第二款涉及的行为也应当成为刑法第三百一十二条的适用范围。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、隐瞒的，应当构成掩饰、隐瞒犯罪所得罪。针对司法实践的具体情形，《危害计算机信息系统安全犯罪解释》第七条第一款规定：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、隐瞒的，违法所得数额在五千元以上的，以掩饰、隐瞒犯罪所得罪追究刑事责任。第二款规定违法所得数额在五万元以上的，应当认定为“情节严重”。针对单位犯罪的情形，第三款专门规定单位犯罪的，定罪量刑标准依照自然人犯罪的定罪量刑标准执行。

需要说明的是，《刑法》第三百一十二条规定的“犯罪所得”过去多限于财产、物品等，将其适用于计算机信息系统数据、控制权，是否可行，有关方面认识不一。本书认为，计算机信息系统数据、控制权可以成为掩饰、隐瞒犯罪所得罪的犯罪对象。主要有如下考虑：一是计算机信息系统数据、控制权是一种无形物，属于“犯罪所得”的范畴，理应成为掩饰、隐瞒犯罪所得罪的对象。将计算机信息系统数据、控制权解释为犯罪所得，符合罪刑法定原则。二是从刑法体系看，《刑法》第三百一十二条的掩饰、隐瞒犯罪所得罪的上游犯罪应该涵盖第一百九十一条洗钱罪规定的上游犯罪以外的所有犯罪，理应适用于危害计算机信息系统安全犯罪。三是作出这种解释，也是司法实践的现实需要。从危害计算机信息系统安全犯罪的现状来看，掩饰、隐瞒计算机信息系统数据、控制权的现象十分突出，不予以打击将无法切断危害计算机信息系统安全犯罪的利益链条，难以切实保障计算机信息系统安全。

（2）以单位名义或者单位形式实施危害计算机信息系统安全犯罪的处理规则。

《危害计算机信息系统安全犯罪解释》第八条规定：“以单位名义或者单位形式实施危害计算机信息系统安全犯罪，达到本解释规定的定罪量刑标准的，应当依照《刑法》第二百八十五条、第二百八十六条的规定追究直接负责的主管人员和其他直接责任人员的刑事责任。”

2015年《刑法修正案（九）》出台，分别在《刑法》第二百八十五和第二百八十六条之后增加一款，作为各自的第四款，其内容就是对单位犯罪加以规范。《刑法》第二百八十五条第四款：“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，依照各该款的规定处罚。”第二百八十六条第四款：“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。”并且在其他针对网络犯罪增设的发条中也都加入了对单位犯罪的规范。《刑法修正案（九）》的这些修改，实际上是将《危害计算机信息系统安全犯罪解释》中已有的对单位作为犯罪主体的情形

① 黄太云.《刑法修正案（六）》的理解与适用（下）.人民检察，2006（15）

所作的规范，正式列入《刑法》。因此，在基本的处理规则上，《危害计算机信息系统安全犯罪解释》关于单位犯罪自动失效，以《刑法修正案(九)》新修改之内容为准。

(3) 危害计算机信息系统安全共同犯罪的处理规则。

《危害计算机信息系统安全犯罪解释》第九条规定："明知他人实施刑法第二百八十五条、第二百八十六条规定的行为，具有下列情形之一的，应当认定为共同犯罪，依照刑法第二百八十五条、第二百八十六条的规定处罚：(一)为其提供用于破坏计算机信息系统功能、数据或者应用程序的程序、工具，违法所得五千元以上或者提供十人次以上的；(二)为其提供互联网接入、服务器托管、网络存储空间、通信传输通道、费用结算、交易服务、广告服务、技术培训、技术支持等帮助，违法所得五千元以上的；(三)通过委托推广软件、投放广告等方式向其提供资金五千元以上的。实施前款规定行为，数量或者数额达到前款规定标准五倍以上的，应当认定为刑法第二百八十五条、第二百八十六条规定的'情节特别严重'或者'后果特别严重'。"

① 网络犯罪的分工细化与利益链条。

网络犯罪一个极为重要的特点就是犯罪活动分工细化，并逐步形成由各个作案环节构成的利益链条，这是网络犯罪泛滥的主要原因之一。

以危害计算机信息系统安全犯罪为例，为危害计算机信息系统违法犯罪行为提供用于破坏计算机信息系统功能、数据的程序，提供互联网接入、服务器托管、网络存储空间、通信传输通道、费用结算、交易服务、广告服务、技术培训、技术支持等帮助，通过委托其推广软件、投放广告等方式向其提供资金等行为十分突出，行为人从中牟取了巨大利益，也使得实施危害计算机信息系统安全犯罪活动的"技术门槛"日益降低。例如，在司法实践中，很多实施危害计算机信息系统安全犯罪活动的行为人只有初中文化程度，其往往是通过购买用于破坏计算机信息系统功能、数据的程序、工具或者获取技术帮助进而实施危害计算机信息系统安全犯罪的。再如，通过互联网搜索引擎可以发现，黑客培训广告已经漫天遍野。可以说，危害计算机信息系统安全犯罪活动分工细化和进而形成的利益链条，导致了危害计算机信息系统安全犯罪活动迅速蔓延。

② 利益链条的打击与共同犯罪处理的疑难。

打击危害计算机信息系统安全犯罪的关键是要斩断利益链。立足现行刑法规定，对于利益链条的打击主要靠适用共同犯罪的有关规定。然而，在网络环境下，共同犯罪具有殊于传统共犯的特性。在传统犯罪中，一个人通常只能是一个或者数个人的共犯。而在网络犯罪中，一个人往往能够成为很多人的共犯。例如，用于破坏计算机信息系统功能、数据的程序、工具的制造者，可以向数以万计甚至更多的破坏计算机信息系统行为人提供程序、工具，成为破坏计算机信息系统实行行为的帮助犯。在这种背景下，一方面，要求抓获所有接受帮助行为的实行犯并查清相关情况，在司法实践中不具有可操作性。以提供程序、工具的帮助为例，提供者通常是以层层代理的方式销售，规模庞大，要查清每个销售出去的程序和工具是否被用于实施网络攻击几乎是不可能的，获利最大的提供者很容易逃避打击。另一方面，

可能存在所有的实行行为均未达到入罪标准，但帮助犯由于向数以万计实行行为提供了帮助，其行为性质非常严重的情况，对此具有刑罚必要性。例如，行为人开发了程序，并将这个程序通过层层代理的方式销售。依据传统的共同犯罪理论，只有使用犯罪工具的人，也就是通常所说的实行犯构成犯罪，才能对帮助犯予以刑事处罚，假如使用这些程序的人员实施的行为不够刑事处罚，则无法将提供者作为共犯处理。

③ 网络共同犯罪疑难的司法应对。

网络共同犯罪的问题非常复杂，但是这种现象又非常普遍，必须予以解决，才能妥善处理网络犯罪刑事法律适用的问题。从刑法、司法解释、规范性文件的相关规定来看，解决网络共同犯罪的问题，主要有三种途径：

第一，将为实施网络犯罪提供帮助的行为，也就是网络犯罪帮助行为独立规定为犯罪，规定单独的定罪量刑标准。这是最为理想的一种解决方式，也是适用中最无争议的方式。实际上，立法已经尝试在这方面努力了。针对非法获取计算机信息系统数据、控制计算机信息系统犯罪中提供犯罪工具的现象十分突出的情况，《刑法修正案(七)》在《刑法》第二百八十五条中第三款增设了独立的提供侵入、非法控制计算机信息系统的程序、工具罪。《刑法修正案(七)》通过立法的方式实现了“共犯行为独立化”，将本来是非法获取计算机信息系统数据、控制计算机信息系统犯罪中的帮助行为独立化，作为单独的犯罪处理。

第二，通过司法解释明确对一些网络帮助犯罪行为按照独立的犯罪处理。由《刑法》将网络共同犯罪独立化，规定单独的罪名，是解决网络共同犯罪问题最为理想的方式。但是，在立法统一修改前，有些时候还得依靠司法解释来明确其中的相关问题。例如，《淫秽电子信息犯罪解释(二)》第四条至第六条规定对有关行为按照《刑法》第三百六十二条、三百六十三条规定的独立犯罪处理。而此前，《淫秽电子信息犯罪解释》规定对这些行为按照共同犯罪处理，但是，实践证明，对这些行为适用共同犯罪处理存在操作困难。因此，《淫秽电子信息犯罪解释(二)》作了扩大解释，明确对这些行为按照独立的犯罪处理。通过制定司法解释的方式，明确对一些网络帮助犯罪行为按照独立犯罪处理，也是一种比较理想的方式，但必须符合刑法的相关规定，符合罪刑法定原则的要求。

第三，作为共同犯罪处理，但是规定单独的定罪量刑标准。实践中存在一些网络帮助犯罪行为，刑法既没有将其独立规定为单独的犯罪，也无法通过扩大解释的方式将其解释为独立犯罪。针对这些情形，有关司法解释和规范性文件专门规定了独立的定罪量刑标准。

例如，《淫秽电子信息犯罪解释(二)》第七条规定，实施通过投放广告等方式向淫秽网站直接或者间接提供资金，或者提供费用结算服务行为，构成制作、复制、出版、贩卖、传播淫秽物品牟利罪的共同犯罪，但是设置了独立的标准：第(一)项以提供资金的网站数量为标准，即向十个以上淫秽网站投放广告或者以其他方式提供资金的构成犯罪；第(二)项以投放广告数量为标准，即向淫秽网站投放广告在二十条以上的构成犯罪；第(三)项以向其提供费用结算服务的淫秽网站数量为标准，即向十个以上淫秽网站提供费用结算服务的构成犯罪；第(四)项以提供资金的数量为标准，即以投放广告或者其他方式向淫秽网站提供资金数额

在五万元以上的构成犯罪；第(五)项以提供费用结算服务所收取服务费数额为标准，即为淫秽网站提供费用结算服务，收取服务费数额在二万元以上的构成犯罪；第(六)项是关于兜底条款的规定。

《网络赌博犯罪意见》第二条“关于网上开设赌场共同犯罪的认定和处罚”规定，明知是赌博网站，而为其提供下列服务或者帮助的，属于开设赌场罪的共同犯罪，依照《刑法》第三百零三条第二款的规定处罚：

第一，为赌博网站提供互联网接入、服务器托管、网络存储空间、通讯传输通道、投放广告、发展会员、软件开发、技术支持等服务，收取服务费数额在二万元以上的；

第二，为赌博网站提供资金支付结算服务，收取服务费数额在一万元以上或者帮助收取赌资二十万元以上的；

第三，为十个以上赌博网站投放与网址、赔率等信息有关的广告或者为赌博网站投放广告累计一百条以上的。

④ 危害计算机信息系统安全共同犯罪的处理。

基于宽严相济刑事政策的考量，按照《淫秽电子信息犯罪解释(二)》第七条、《网络赌博犯罪意见》第二条的思路，《危害计算机信息系统安全犯罪解释》对于共犯的成立设置了独立的定罪量刑标准，对情节严重的行为予以刑事惩治。其第九条的目的就是打击黑客攻击破坏活动相关利益链条：由于《刑法》二百八十五条第三款将明知他人实施侵入、非法控制计算机信息系统而向其提供程序、工具的行为入罪，而对于“明知他人实施破坏计算机信息系统功能或者数据的犯罪行为，而为其提供用于破坏计算机信息系统功能、数据或者应用程序的程序或者工具”的行为并未单独入罪处罚，第(一)项将其作为共犯处理；第(二)项将向危害计算机系统安全行为提供帮助获利的行为作为共犯处理；第(三)项将从危害计算机信息系统安全行为获得帮助并向其提供资金的行为作为共犯处理。

在司法适用过程中，需要注意如下两个问题：

第一，跨国共同犯罪的处理问题。由于网络的无国界，危害计算机信息系统安全犯罪行为和犯罪结果可能分别发生在中华人民共和国领域内外。根据《刑法》第六条的规定，犯罪的行为或者结果有一项发生在中华人民共和国领域内的，就认为是在中华人民共和国领域内犯罪。因此，对于这类危害计算机信息系统安全犯罪案件，只要其危害后果最终发生在中华人民共和国领域内，应当认为是在中华人民共和国领域内犯罪，应当适用我国刑法的相关规定。在此前提下，可能对境外实行犯无法实际行使刑事管辖权，在境外实行犯未归案的情况下，对于为境外实行犯提供帮助的境内行为人，应当依照本条确定的规则处理。

第二，帮助犯在共同犯罪中的类型认定问题。与传统犯罪不同，网络环境中的帮助犯在共同犯罪中所起的作用具有一定的特殊性和复杂性，并非只起次要和辅助作用，也可能起主要作用。因此，对于行为人帮助他人实施《刑法》第二百八十五条、第二百八十六条规定的行为的，应当根据其在共同犯罪中的作用予以认定，既可以认定为主犯，也可以认定为从犯。

3.3 计算机网络作为犯罪工具的法律规制

1997年,《中华人民共和国刑法》增加第二百八十七条“利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的,依照本法有关规定定罪处罚”。目的是打击以网络作为工具的犯罪活动:2015年,《中华人民共和国刑法修正案(九)》在第二百八十六条中新增两个罪名;“非法利用信息网络罪”和“帮助信息网络犯罪活动罪”①。除此之外,《刑法》中还有第二百八十八条和第二百九十一条的关于网络作为工具的犯罪的法律规定。这些案件统称为“涉网犯罪”。

3.3.1 计算机网络作为工具的犯罪定性

1997年,《刑法》第二百八十七条规定:“利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的,依照本法有关规定定罪处罚。”该条强调以“计算机”作为犯罪工具实施诈骗、盗窃等传统犯罪的,仍然应当依照刑法规定定罪量刑。而随着网络的发展,计算机逐渐融入网络之中。因此可以认定《刑法》第二百八十七条就是针对传统犯罪的网络化。

对此,不能作如下理解:对于利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪,属于牵连犯,《刑法》第二百八十七条已对此做出了特别规定,对此种情况只能依据目的行为或者结果行为所触犯的罪名定罪处罚,司法实践中无须再判断重罪,应当直接适用目的行为或者结果行为所涉及的罪名。如果作这种理解,在通过实施危害计算机信息系统安全犯罪进而实施敲诈勒索、破坏生产经营等犯罪的情形下,可能会出现罪刑失衡的问题。例如,在2011年4月30日之前,行为人通过实施拒绝服务攻击,对他人实施敲诈勒索的,结果导致出现了大规模网络瘫痪的情况。此种情况下,如果按照敲诈勒索罪定罪处罚,最高只能处十年有期徒刑,而如果按照破坏计算机信息系统罪定罪处罚,最高可以处十五年有期徒刑。更为极端的情况是,行为人实施拒绝服务攻击行为,以实现破坏他人生产经营的目的,按照破坏生产经营罪最高只能处七年以下有期徒刑,更为不合理。因此,此种情况下,仍然应依据刑法理论和刑法规定,按照“从一重处断”原则处理,以免出现将《刑法》第二百八十六条规定的“破坏计算机信息系统罪”作为网络时代“口袋罪”,造成罪刑的失衡。

但是,司法实践的发展和法律最初制定时的设计难免有背道而驰的现象发生。目前,只要涉及计算机或者网络的案件,在司法实践中似乎出现了“破坏计算机信息系统罪”就是唯一的定性选择的潜规则,《刑法》第二百八十六条在事实上已经逐渐成为“口袋罪”,囊括了所有涉网的传统犯罪行为。而《刑法》第二百八十七条在1997年制定之初,实际上是指向未来

① 《最高人民法院、最高人民检察院关于执行〈中华人民共和国刑法〉确定罪名的补充规定(六)》。

可能出现的犯罪形态的预测性条款。因此在当时的技术背景下，只是以“计算机”一词泛指各类新工具，而并没有使用“网络”这一措辞，造成因时代背景而留下的法条遗憾，也推高了这一罪名的司法适用概率。

为此，2000 年 12 月 28 日全国人大常委会会议通过的《关于维护互联网安全的决定》，对网络作为“犯罪工具”的整体犯罪态势和趋势进行专门的整体解释。整部决定共含七条，实际上就是对网络作为“犯罪工具”时的传统犯罪定性问题。

随着网络犯罪形态的不断更新，刑法亟须更新，需要不断完善相关规定，才能保持对网络犯罪的高压态势，因此 2015 年 8 月 29 日，全国人大通过《中华人民共和国刑法修正案(九)》，其中的重要部分是对网络犯罪的刑法规定作出完善性修改。对于以计算机网络为工具的犯罪活动的规定主要有以下方面[①]：

(1) 修改侮辱罪、诽谤罪的告诉才处理规定。规定通过信息网络实施侮辱、诽谤行为，被害人向人民法院告诉，但提供证据确有困难的，人民法院可以要求公安机关提供协助。

(2) 针对网络犯罪预备行为独立入罪，根据网络犯罪“打早打小”的策略要求，有针对性地对尚处于预备阶段的网络犯罪行为独立入刑处罚，规定利用信息网络实施以下行为之一，情节严重的，构成犯罪：

① 设立用于实施诈骗、传授犯罪方法、制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组的；

② 发布有关制作或者销售毒品、枪支、淫秽物品等违禁物品、管制物品或者其他违法犯罪信息的；

③ 为实施诈骗等违法犯罪活动发布信息的。

(3) 针对网络犯罪帮助行为独立入罪。打击网络犯罪的关键是斩断利益链，针对帮助网络犯罪多发的情况，将明知他人利用信息网络实施犯罪，为其犯罪提供互联网接入、服务器托管、网络存储、通信传输等技术支持，或者提供广告推广、支付结算等帮助，情节严重的规定为犯罪。

(4) 修改扰乱无线电通信管理罪。针对开设“伪基站”等设备严重扰乱无线电秩序、侵犯公民权益的情况，取消“经责令停止使用拒不停止使用的”要件，增加可操作性。同时，由结果犯调整为情节犯，将“干扰无线电通讯正常进行，造成严重后果”的入罪要件修改为“干扰无线电通讯秩序，情节严重”，并针对“情节特别严重的”情形增加规定“处三年以上七年以下有期徒刑，并处罚金”。

(5) 增加编造、故意传播虚假信息罪。将编造虚假的险情、疫情、灾情、警情，在信息网络或者其他媒体上传播，或者明知是上述虚假信息，故意在信息网络或者其他媒体上传播，严重扰乱社会秩序的行为规定为犯罪。

---

① 喻海松. 刑法的扩张《刑法修正案(九)》及新近刑法立法解释司法适用解读. 北京：人民法院出版社，2015

3.3.2 计算机网络作为工具的犯罪立法要点

对于以计算机网络为工具的犯罪活动，要重点把握以下几个立法方面，才能准确把握打击力度，做到有效打击。

2015年，《刑法修正案(九)》出台，将部分对传统犯罪行为的规范进行了扩张解释，以法条的形式呈现出来，以避免司法实践中对相关行为认定时出现的混乱。而这些行为也恰恰是近几年多发的犯罪行为，并且常常会因适用法律不明而在司法实践中带来困惑。

根据《刑法修正案(九)》的规定，在《刑法》第二百八十七条之后增加两条，作为第二百八十七条之一和第二百八十七条之二；在第二百八十九条之一中增加一款作为第二款。

其中第二百八十七条之一规定：利用信息网络实施下列行为之一，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金：(一)设立用于实施诈骗、传授犯罪方法、制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组的；(二)发布有关制作或者销售毒品、枪支、淫秽物品等违禁物品、管制物品或者其他违法犯罪信息的；(三)为实施诈骗等违法犯罪活动发布信息的。单位犯前款罪的，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。有前两款行为，同时构成其他犯罪的，依照处罚较重的规定定罪处罚。

第二百八十七条之二规定：明知他人利用信息网络实施犯罪，为其犯罪提供互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者提供广告推广、支付结算等帮助，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金。单位犯前款罪的，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。有前两款行为，同时构成其他犯罪的，依照处罚较重的规定定罪处罚。

第二百八十九条之一第二款：编造虚假的险情、疫情、灾情、警情，在信息网络或者其他媒体上传播，或者明知是上述虚假信息，故意在信息网络或者其他媒体上传播，严重扰乱社会秩序的，处三年以下有期徒刑、拘役或者管制；造成严重后果的，处三年以上七年以下有期徒刑。

这些行为所侵犯的利益及其行为的本质，已经是其他传统犯罪所涵盖的情形之内。但是由于在网络空间中，这些行为的方式、模式和对其社会危害性的评价标准都发生了网络异化。因此，上述法条实际上是对传统犯罪行为规范的扩张解释。要正确理解这些法条，还是需要在新的时代背景下对传统犯罪行为进行重新思考和合理解释。

实际上，在《刑法修正案(九)》之前，一系列司法解释和规范性文件就是在针对相关传统犯罪在向网络空间迁移的过程中出现的新问题，对相关法条及其中的关键词进行解释。下面，本节将对几个具体的法律文件的出台背景和主要意图进行简要介绍。

3.3.3 《关于办理网络赌博犯罪案件适用法律若干问题的意见》

针对网络赌博犯罪高发的问题，为加大打击力度，最高人民法院、最高人民检察院于

2005 年出台了《关于办理赌博刑事案件具体应用法律若干问题的解释》，在 2010 年整治网络赌博专项行动期间，最高人民法院、最高人民检察院、公安部联合出台了《关于办理网络赌博犯罪案件适用法律若干问题的意见》。

《关于办理网络赌博犯罪案件适用法律若干问题的意见》（本节以下简称《意见》）主要解决了下述问题：

一是进一步明确“开设赌场”行为的范围。针对很多机构设立赌博网站但自身并不接受投注，而是通过出租平台获利，以及有的人员通过向赌博网站投资，但不直接参与经营的情况，将“建立赌博网站并提供给他人组织赌博”和“参与赌博网站利润分成”的行为也认定为“开设赌场行为”。

二是明确了开设赌场罪“情节严重”的情形。在《意见》中参照 2005 年出台的司法解释中的定罪量刑标准，将抽头渔利数额、赌资数额、参赌人数数量达到“聚众赌博”罪有关标准 5 倍以上的认定为“情节严重”。此外，还新增了“违法所得”等 5 款认定标准。

三是明确了打击网络赌博相关利益链条适用法律的依据。对明知是赌博网站，而为其提供服务器托管、投放广告、资金结算等帮助的行为明确了定罪量刑标准，同时明确了 4 种应当认定为明知的情形，例如有的第三方支付平台为了吸纳赌博业务，给赌博网站流转资金收取费率下调，这种收取服务费明显异常的行为应当认定为明知，再如有的门户网站、搜索引擎投放赌博网站网址、赔率等广告，在公安机关书面告知后没有采取有效措施，仍继续实施上述行为的，应当认定为明知。

四是明确了参赌人数、赌资数额和网站代理的认定依据。也即网站显示的账户数和银行汇款账户数可以直接认定为参赌人数，无须逐一查实参赌人员；对于用于收取、流转赌资的账户中的资金，如果嫌疑人不能说明资金合法来源的，应当认定为赌资，也即将举证责任倒置，由嫌疑人负责举证资金的合法性。

五是解决了网络赌博犯罪案件的管辖问题。其基本原则是网络赌博所涉及所有要素所在地都具有管辖权，且对于已提请审查逮捕、移送起诉或者进入审判程序的案件，对于存在管辖异议的，原则上不再移送其他地方，而由检、法部门向上级申请指定管辖。在适用这一条中要特别注意这并不意味着侦查机关可以任意到异地办理网络赌博案件，例如本地有参赌人员，可以到异地追查其直接代理、代理的直接上级股东等（也即可以顺线上追查，因为自上往下的一个组织链条与本地的参赌人员的赌博活动有关系），但如果扩线又发现其他代理，但这些代理组织的网络赌博并不涉及本地的，则应当移交异地侦查机关处理。

3.3.4　《关于办理利用互联网移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释》

针对网络淫秽色情犯罪高发的问题，为加大打击力度，最高检、最高法于 2004 年和 2010 年出台了《关于办理利用互联网移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫

秽电子信息刑事案件具体应用法律若干问题的解释》和《关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释(二)》两个司法解释。

1. 司法解释一解决了传播淫秽物品适用法律的主要问题

一是从传播淫秽物品的数量、点击数量、注册会员数量、违法所得数额等方面确定了定罪量刑标准;

二是对于明知是淫秽信息而在自己管理的网站上提供直接链接的行为按照传播淫秽信息的行为定罪处罚;

三是对传播儿童色情信息、向未成年人传播淫秽物品、通过恶意代码强制用户访问淫秽信息等行为作为从重处罚的情节;

四是对明知他人传播淫秽物品而为其提供帮助的行为,明确以共同犯罪论处。

2. 司法解释二解决的主要问题

一是针对设立主要用于传播淫秽电子信息的群组,明确成员达到 30 人以上的,即以传播淫秽物品罪定罪处罚;

二是对于明知是淫秽电子信息而放任他人在自己网站上发布淫秽信息的行为,明确按照传播淫秽物品罪定罪处罚,比如某个网站或者搜索引擎上频繁出现淫秽信息,在公安机关书面告知后仍没有采取有效措施导致淫秽信息仍然在其网站或者搜索引擎上蔓延,则应当依法定罪处罚;

三是明确传播淫秽儿童色情信息行为从重处罚的定罪量刑标准,将传播儿童色情信息的定罪数量降为一般淫秽信息的一半;

四是对网络淫秽色情活动提供帮助的利益链条确定独立的定罪量刑标准:一方面是对从淫秽色情活动获利的利益链条明确定罪量刑标准,也即对于明知是淫秽网站,仍为其提供互联网接入、网络存储空间、代收费等帮助并收取费用,按照传播淫秽物品牟利罪定罪处罚;另一方面是对为淫秽色情活动提供资金的利益链条确定定罪量刑标准,以打击网络淫秽色情活动的经济来源,对于明知是淫秽网站而通过向其投放广告等方式向其直接或者间接提供资金,或者提供费用结算服务的行为按照传播淫秽物品牟利罪的共同犯罪处罚;

五是明确了认定为“明知”的几种情形,包括在行政主管机关书面告知后仍然实施“上述行为”“接到举报后不履行法定管理职责的”等五种情形。

3.3.5 《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》

最高人民法院、最高人民检察院于 2013 年 9 月 10 日发布《最高人民法院、最高人民检察院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》,该解释共有十条,主要规定了八个方面的内容。

(1) 明确了利用信息网络实施诽谤犯罪的行为方式,即“捏造事实诽谤他人”的认定

问题；

（2）明确了利用信息网络实施诽谤行为的入罪标准，即“情节严重”的认定问题；

（3）明确了利用信息网络实施诽谤犯罪适用公诉程序的条件，即“严重危害社会秩序和国家利益”的认定问题，共列举了七种情形：

① 引发群体性事件的；

② 引发公共秩序混乱的；

③ 引发民族、宗教冲突的；

④ 诽谤多人，造成恶劣社会影响的；

⑤ 损害国家形象，严重危害国家利益的；

⑥ 造成恶劣国际影响的；

⑦ 其他严重危害社会秩序和国家利益的；

（4）明确了利用信息网络实施寻衅滋事犯罪的认定问题；

（5）明确了利用信息网络实施敲诈勒索犯罪的认定问题；

（6）明确了利用信息网络实施非法经营犯罪的认定及处罚问题；

（7）明确了利用信息网络实施诽谤、寻衅滋事、敲诈勒索、非法经营等犯罪的共同犯罪内容；

（8）明确了利用信息网络实施诽谤、寻衅滋事、敲诈勒索、非法经营犯罪与其他犯罪的数罪问题及其处罚原则。

3.4　网络犯罪的刑事程序法律规制

2012 年 3 月 14 日，第十一届全国人民代表大会第五次会议通过《关于修改〈中华人民共和国刑事诉讼法〉的决定》，并于 2013 年 1 月 1 日起施行，完成了对《刑事诉讼法》的第二次修改。

新修改的《刑事诉讼法》进一步完善了涉及网络犯罪刑事诉讼程序的相关规定，特别是将电子数据增设为新的证据种类。此外，有关司法解释、规范性文件也进一步明确了网络犯罪的法律适用问题，如《网络赌博犯罪意见》对网络赌博犯罪案件的管辖、电子证据的收集与保全等问题作了专门规定。

但是总体而言，由于网络犯罪与传统犯罪有着很大的差异，特别是网络犯罪的跨地域性、技术性、分工合作等特点，传统办案程序相关规定直接适用于网络犯罪案件尚存在很多不适应的地方，为配合修改后的《刑事诉讼法》顺利实施，进一步明确网络违法犯罪案件的办案程序，最高人民法院、最高人民检察院、公安部于 2014 年 5 月 6 日印发了《关于办理网络犯罪案件适用刑事诉讼程序若干问题的意见》（公通字[2014]10 号，以下简称《网络犯罪刑事诉讼程序意见》），解决了近年来公安机关、人民检察院、人民法院在办理网络犯罪案件程序上遇到的新情况、新问题，为依法惩治网络犯罪活动提供有力的保障。

《网络犯罪刑事诉讼程序意见》主要解决了以下几个问题。

1. 明确案件管辖

计算机网络具有跨地域特性，相应的网络犯罪也存在跨地域特性，与犯罪相关的人员（被害人、嫌疑人）以及相关的资源（银行账户、虚拟身份、网站）等基本要素分布在不同的地方。如在网络赌博、传销等案件中，嫌疑人通过层层发展下线形成金字塔型的组织结构，涉及全国多地，且人数众多。此类案件中，由于法律缺乏明确规定，导致有关机关常因管辖权问题产生争议。《网络犯罪刑事诉讼程序意见》明确了网络犯罪案件的管辖原则，包括争议处理原则，并案处理原则，涉众型网络犯罪案件的并案管辖原则，跨地重大网络犯罪案件的异地指定管辖原则，网络犯罪案件的合并处理原则，已受理的网络犯罪案件发现没有管辖权的处理原则以及网络共同犯罪的先行追诉及后到案犯罪嫌疑人、被告人的管辖原则。特别是针对网络犯罪案件与传统案件的区别，规定了网络犯罪案件涉及多个犯罪地或者多个犯罪环节的管辖如何确定，规定了可以并案侦查的情形以及犯罪利益链顶端的犯罪分子由谁打击等问题，同时也规定了具备侦查管辖公安机关同级检察院、法院的管辖问题，为减少办案过程中推诿扯皮扫清了障碍。

2. 立案前可采取初查

刑事诉讼法对刑事立案前公安机关可以采取的调查措施未作明确规定。然而，大量的网上违法犯罪线索如不经过调查则很难确定是否达到立案标准，如网上发布信息声称销售枪支、毒品，如未进行调查则无法确定是否存在销售枪支的事实，难以立案。这一问题致使大量网上违法犯罪线索难以进入侦查程序，使得很多违法犯罪嫌疑人肆无忌惮地发布销售违禁品的信息。当前，互联网上销售枪支、毒品、个人信息、窃听器材、人体器官等违禁品的网站和信息泛滥，但公安机关难以对犯罪嫌疑人开展打击，致使这些违法信息在互联网上大肆蔓延，屡删屡发，人民群众反应非常强烈。因此《网络犯罪刑事诉讼程序意见》对网络犯罪案件立案前的调查措施作出规范，检法部门认可公安机关在初查阶段收集的证据，《网络犯罪刑事诉讼程序意见》明确，对接受的案件或者发现的犯罪线索，在审查中发现案件事实或者线索不明，需要经过调查才能够确认是否达到犯罪追诉标准的，经办案部门负责人批准，可以进行初查，同时在《网络犯罪刑事诉讼程序意见》中明确了初查的内容以及程序规定。

3. 跨地域取证困难

网络犯罪相关网络数据、银行账户等要素分布在不同地方，动辄涉及全国各地，根据传统取证程序，通常需要办案地派民警携带法律文书到证据所在地开展证据调取工作，工作量巨大，难以有效调取相关证据。特别是，行为人通常借助计算机网络对不特定人实施侵害或者组织不特定人实施犯罪，被害人和涉案人员众多，公安机关难以逐一取证认定被害人数、被侵害计算机信息系统数、违法所得等犯罪事实。例如，2011 年某地公安机关侦办一起网络诈骗案件，被骗万余人分布在全国各地，每位被害人被骗金额 100～2000 元不等，无法对所有被害人逐一取证认定被害人数以及诈骗数额。这一问题严重制约对网络诈骗等网络侵财犯罪的打击。目前，网络诈骗每年发案数量达数十万起，占网络犯罪发案数量的 80％以

上，人民群众反映十分强烈。《网络犯罪刑事诉讼程序意见》根据实践中的具体情况，专门对跨地域取证的有关问题作了规定，创新了办理网络犯罪案件中跨地域取证的方式，即可以通过信息化系统传输相关法律文书或者通过远程网络视频等方式询(讯)问。

3.5　网络犯罪的电子数据证据法律规制

1996 年刑事诉讼法第四十二条规定了“书证、物证”等七类证据，并未将电子数据列为证据的种类，这导致司法实践中对电子数据的运用处于两难境地：一方面，可以用于证明案件事实的材料都是证据，尽管网络犯罪案件中也涉及书证、物证等传统证据，但是更多的是电子数据，与案件相关的电子数据自然属于证据的范畴；另一方面，作为大陆法系，1996 年刑事诉讼法又将证据限定为七种，并未涉及电子数据，电子数据应当作为何种类的证据于法无据。这就使得电子数据的地位极为尴尬，与网络犯罪打击的迫切需要形成巨大矛盾。

面对这一局面，刑事司法实践部门采取了两类举措。一类举措是在规范性文件中直接将电子数据作为一类证据形式。例如，《关于办理死刑案件审查判断证据若干问题的规定》在“证据的分类审查与认定”部分直接规定了对电子邮件、电子数据交换、网上聊天记录、网络博客、手机短信、电子签名、域名等电子证据的审查内容。另一类举措则是将电子数据转化为法定证据种类再予以使用，而且不少都是转化为勘验、检查笔录予以使用。例如，《网络赌博犯罪意见》在“关于电子证据的收集与保全”部分规定：“侦查机关对于能够证明赌博犯罪案件真实情况的网站页面、上网记录、电子邮件、电子合同、电子交易记录、电子账册等电子数据，应当作为刑事证据予以提取、复制、固定。侦查人员应当对提取、复制、固定电子数据的过程制作相关文字说明，记录案由、对象、内容以及提取、复制、固定的时间、地点、方法，电子数据的规格、类别、文件格式等，并由提取、复制、固定电子数据的制作人、电子数据的持有人签名或者盖章，附所提取、复制、固定的电子数据一并随案移送。”从这一规定可以看出，该规范性文件实际上是要求对电子数据按照勘验、检查笔录这一法定证据种类进行提取和转换的。以上两类举措都是司法实务部门囿于电子证据未作为法定证据种类，不得已而为之的举措。

2012 年修改的《刑事诉讼法》将电子数据纳入法定的证据种类，首次赋予电子数据证据独立的法律地位。这一修改，使《刑事诉讼法》适应网络时代的发展，根据刑事诉讼中出现的新情况和实践需要，将电子数据增设为法定证据种类，进一步丰富了证据的外延，有利于规范司法实务部门对于电子数据的提取和运用，能够更好地证明案件事实。

《刑事诉讼法》第四十八条规定：

可以用于证明案件事实的材料，都是证据。

证据包括：

（一）物证；

（二）书证；

（三）证人证言；

（四）被害人陈述；

（五）犯罪嫌疑人、被告人供述和辩解；

（六）鉴定意见；

（七）勘验、检查、辨认、侦查实验等笔录；

（八）视听资料、电子数据。

证据必须经过查证属实，才能作为定案的根据。

随后《民事诉讼法》《行政诉讼法》均将“电子数据”作为证据类型予以确定。因此电子数据是一类独立的证据种类。

3.5.1 电子数据的取证程序规则

虽然刑事诉讼法已明确将电子数据作为新的法定证据类型，但对于电子数据的提取、固定、出示、辨认、质证等活动缺乏明确的规定，主要存在四个方面的突出问题。一是由于电子数据具有易篡改性，缺乏明确的电子数据取证程序规范，将导致电子数据的完整性、真实性受到质疑，进而影响电子数据的证明力。二是很多电子数据无法通过扣押原始存储介质的方式进行取证，也无法通过重复取证过程展现电子数据的原始性。例如，境外主机上存储的信息无法通过扣押计算机机器存储介质的方式进行取证，计算机内存中存储的数据一旦主机关机即会丢失，对于此类电子数据的取证程序和要求应当进一步予以明确，否则会影响电子数据的证明力。三是不少电子数据是传统书证、音视频证据的电子化形式，对于此类可以直接展示的电子数据应当以何种形式展示、使用缺乏明确的规定。四是很多电子数据无法直接展示，如计算机病毒程序、网站代码、网络攻击日志等电子数据无法通过直接展示的方式说明其所证明的事实，对于此种电子数据应当如何使用，须作进一步明确规定。

《网络犯罪刑事诉讼程序意见》明确了电子数据取证的基本原则与程序，规定了电子数据的提取方式、笔录内容、电子数据展示方式以及取证人员、机构应具备的资质、条件等内容。《网络犯罪刑事诉讼程序意见》是电子数据成为合法证据类型以来首个明确电子数据取证程序的规范性文件。

例如对于电子数据取证人员和设备的要求。《网络犯罪刑事诉讼程序意见》第十三条规定：“收集、提取电子数据，应当由二名以上具备相关专业知识的侦查人员进行。取证设备和过程应当符合相关技术标准，并保证所收集、提取的电子数据的完整性、客观性。”

对于电子数据原始性也有具体要求，第十四条规定：“收集、提取电子数据，能够获取原始存储介质的，应当封存原始存储介质，并制作笔录，记录原始存储介质的封存状态，由侦查人员、原始存储介质持有人签名或者盖章；持有人无法签名或者拒绝签名的，应当在笔录中注明，由见证人签名或者盖章。有条件的，侦查人员应当对相关活动进行录像。”

对于电子数据的检验鉴定，第十八条规定：“对电子数据涉及的专门性问题难以确定的，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检验报告。”

3.5.2　电子数据的证据审查规则

与传统证据的实物性或者言词性不同，电子数据具有虚拟性的特点，因此，对电子数据的收集是一个需要特别注意和把握的问题，要注意合技术性和合法律性两个方面的要求。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》（法释[2012]21 号）对审查电子数据的一般原则和重点内容作出了规范，对电子数据的审查判断作出了规定。

《刑事诉讼法解释》第九十三条规定：

对电子邮件、电子数据交换、网上聊天记录、博客、微博客、手机短信、电子签名、域名等电子数据，应当着重审查以下内容：

（一）是否随原始存储介质移送；在原始存储介质无法封存、不便移动或者依法应当由有关部门保管、处理、返还时，提取、复制电子数据是否由二人以上进行，是否足以保证电子数据的完整性，有无提取、复制过程及原始存储介质存放地点的文字说明和签名；

（二）收集程序、方式是否符合法律及有关技术规范；经勘验、检查、搜查等侦查活动收集的电子数据，是否附有笔录、清单，并经侦查人员、电子数据持有人、见证人签名；没有持有人签名的，是否注明原因；远程调取境外或者异地的电子数据的，是否注明相关情况；对电子数据的规格、类别、文件格式等注明是否清楚；

（三）电子数据内容是否真实，有无删除、修改、增加等情形；

（四）电子数据与案件事实有无关联；

（五）与案件事实有关联的电子数据是否全面收集。

对电子数据有疑问的，应当进行鉴定或者检验。

《刑事诉讼法解释》第九十四条规定：

视听资料、电子数据具有下列情形之一的，不得作为定案的根据：

（一）经审查无法确定真伪的；

（二）制作、取得的时间、地点、方式等有疑问，不能提供必要证明或者作出合理解释的。

具体而言，《刑事诉讼法解释》强调对于电子数据证据应当着重审查以下内容：

（1）电子数据是否随原始存储介质移送。

在原始存储介质无法封存、不便移动或者依法应当由有关部门保管、处理、返还时，提取、复制电子数据是否由二人以上进行，是否足以保证电子数据的完整性，有无提取、复制过程及原始存储介质存放地点的文字说明和签名。

与传统证据种类不同，电子数据没有“原始电子数据”的概念，只有“原始存储介质”的概念。由于电子数据的电子性，电子数据不同于物证、书证等其他证据种类，其可以完全同原始存储介质分离开来。例如，存储在计算机的电子文档，可以同计算机这一存储介质分离开来，存储于移动硬盘、U 盘等存储介质之中。而且，对电子数据的复制可以确保与原数据的完全一致性，复制后的电子数据与原数据没有任何差异。与此不同，物证、书证等证据无法同原始存储介质完全区分开来，更无法采取确保与原物、原件完全一致的方式予以复制。例

如，一封作为书证使用的书信，书信的原始内容无法同原始载体完全分离开来，只能存在于原始的纸张这一载体之上，即使采取彩色复印等方式进行复制，也无法确保复制后的书信同原件的完全一致性。不仅物证、书证等传统证据如此，视听资料这一随着技术发展而兴起的新型证据亦是如此。① 基于上述考虑，使用“原始电子数据”这个概念没有任何意义，对于电子数据而言，不存在“原始电子数据”的概念。但是，电子数据原始存储介质这个概念是有意义的，这表明电子数据是存储在原始的介质之中，即取证时是将存储介质予以扣押，并作为证据移送，而非运用移动存储介质将该电子数据从原始介质中提取，如直接从现场扣押行为人使用的电脑中提取。因此，可以将电子数据区分为电子数据是随原始存储介质移送，还是在无法移送原始存储介质的情况下（如大型服务器中的电子数据）通过其他存储介质予以收集。为了确保随原始存储介质移送的电子数据的真实性、完整性，针对此种情形，审判人员要审查电子数据随原始存储介质移送的，是否采取了技术措施保证原始存储介质数据的完整性，如通过加写保护设备确保数据不被修改。

而在原始存储介质无法封存、不便移动或者依法应当由有关部门保管、处理、返还时，应当审查提取、复制电子数据是否由二人以上进行，是否足以保证电子数据的完整性，有无提取、复制过程及原始存储介质存放地点的文字说明和签名。审判人员应当对上述情况进行审查，以判断未随原始存储介质移送的电子数据的真实性和完整性。特别需要注意的是电子数据完整性的问题。为解决数据的完整性问题，侦查机关可以通过记录电子数据完整性校验值等方式保证电子数据的完整性，完整性校验值是对电子数据计算获得的一组数据，如果原始数据被修改，则完整性校验值必定发生变化。因此，审判人员在审查电子数据的过程中，应当审查侦查机关是否对电子数据采取记录电子数据完整性校验值等方式保证电子数据的完整性。

（2）收集程序、方式是否符合法律及有关技术规范。

经勘验、检查、搜查等侦查活动收集的电子数据，是否附有笔录、清单，并经侦查人员、电子数据持有人、见证人签名；没有持有人签名的，是否注明原因；远程调取境外或者异地的电子数据的，是否注明相关情况；对电子数据的规格、类别、文件格式等注明是否清楚。

收集电子数据的程序、方法无疑应当符合法律，同时，由于电子数据具有较强的技术性，应当特别审查收集过程是否符合有关技术规范的要求，电子数据的形态是否发生改变。而从司法实践来看，侦查机关经常通过勘验、检查、搜查等侦查活动收集犯罪现场的电子数据。因此，对于通过勘验、检查、搜查等侦查活动收集的电子数据的审查与判断，有必要根据该类侦查活动的特点予以规范。

《刑事诉讼法》第一百四十条规定：“对查封、扣押的财物、文件，应当会同在场见证人和被查封、扣押财物、文件持有人查点清楚，当场开列清单一式二份，由侦查人员、见证人和持

① 需要注意的是，这一论断的前提是随着电子数据成为独立的证据种类，以电子数据形式存在的视听资料是电子数据，不再属于视听资料的范畴。

有人签名或者盖章，一份交给持有人，另一份附卷备查。”审查经侦查人员、电子数据持有人、见证人签名的相关笔录或者清单，是核实电子数据真实性和完整性的必要措施。《刑事诉讼法》虽然将电子数据规定为独立的证据种类，但为了确保电子数据的真实性、完整性，须以笔录形式记录现场提取电子数据的过程，以清单形式记录提取电子数据的结果。因此，在审判环节，对于经勘验、检查、搜查等侦查活动收集的电子数据，审判人员应当审查是否附有笔录、清单，并经侦查人员、电子数据持有人、见证人签名，没有持有人签名的，是否注明原因。

需要特别注意的是，如果电子数据位于境外，难以通过国际司法协助获取相关数据，通常通过远程调取的方式获取数据。而且，即使在国内，也可能在个别案件中采取异地远程调取电子数据的情况。此种情况下，应当注明相关情况。审判人员应当根据注明的情况予以审查，判断电子数据提取过程的合法性，判断所提取电子数据的真实性和完整性。

(3) 电子数据内容是否真实，有无删除、修改、增加等情形。

在法庭审查过程中，审判人员应当通过听取控辩双方意见、询问相关人员等多种方式审查电子数据的内容和制作过程的真实性，必要时可以进行庭外调查。但是，由于电子数据的技术性较强，一般的删除、修改、增加等情形难以通过审判人员的观察作出认定，需要外力的辅助。因此，《刑事诉讼法解释》第九十三条第二款规定：“对电子数据有疑问的，应当进行鉴定或者检验。”这里的鉴定或者检验，主要针对的是计算机程序功能(如计算机病毒等破坏性程序的功能)和数据同一性、相似性(如侵权案件需要认定盗版软件与正版软件的同一性、相似性)的问题。[①] 之所以这里没有要求对有疑问的电子数据一律进行鉴定，而是也可以进行检验，主要是基于当前的司法现状。当前，如果在现有条件下要求对所有案件一律出具鉴定意见，不少案件将难以处理。而且，《危害计算机信息系统安全犯罪解释》等司法解释已经规定对于部分特定电子数据可以进行检验。因此，这里基于现实需要，考虑到以往司法解释的规定，对于有疑问的电子数据，既可以采取鉴定的方式，也可以采取侦查机关检验与司法机关认定相结合的方式。对于采取检验方式的，根据《刑事诉讼法解释》第八十七条的规定，应当参照鉴定的有关规定执行，特别是，经人民法院通知，检验人应当出庭作证。经查证属实的，检验报告可以作为定罪量刑的参考。

(4) 电子数据与案件事实有无关联。

通过前述审查，在判断电子数据的合法性和真实性之余，还应当对电子数据与案件事实的关联性进行审查。只有与案件事实有关联的电子数据，才能作为证据使用；不具有关联性的，不应当作为证据使用。

(5) 与案件事实有关联的电子数据是否全面收集。

由于技术原因，电子数据的形式多种多样，涉及面较宽，相应地，涉及案件事实的电子数

---

① 需要注意的是，鉴定或者检验并非审查认定电子数据的前提条件和必经程序。通常而言，只有通过其他方法审查电子数据仍然存在疑问的，才需要进行鉴定或者检验。司法实践中一定程度存在的对电子数据一律要求附有鉴定意见或者检验报告的做法似可商榷。

据的范围也较宽。因此，在司法实践中，要注意全面收集与案件事实有关联的电子数据，避免有所遗漏。要全面审查电子数据，“既要审查存在于计算机软硬件上的电子数据，也要审查其他相关外围设备中的电子数据；既要审查文本信息，也要审查图像、视频等信息；既要审查对犯罪嫌疑人不利的证据，也要审查对其有利的证据，通过全面综合审查，审查电子数据与其他证据之间的关系，确认电子数据与待证事实之间的关系”。[①] 特别是，对于犯罪分子删除或者由于其他原因被删除的电子数据，应当借助一定的技术予以恢复，以更为全面地证明案件事实。

（6）对于采取技术侦查措施收集的电子数据，要按照对技侦证据的相关规定进行审查。

同视听资料一样，侦查机关经过严格的批准手续，可以采取网络技术侦查措施，收集相应的电子数据。对于这类电子数据，除了按照前述的规定审查外，更要注重对合法性进行判断，审查是否经过严格的批准手续，取证过程是否符合法律和有关规定。

3.6 本章小结

网络犯罪将网络作为屏障，具有高度的隐蔽性，演变的种类繁多，特点不一。这都对网络犯罪的法律规制的普适性造成巨大的阻碍，网络犯罪立法总是滞后时代的要求。这要求侦查机关一方面要充分利用法律规定打击网络犯罪活动；一方面要积极协调立法机关，针对现实情况，迅速地制定相关法律法规。侦查机关不仅仅是法律的执行者，而更应该理解立法的精神和方向，并将其运用在实践中。

思 考 题

1. 涉及网络犯罪的刑法修正案有哪些？新增了什么罪名？

2. 网络犯罪的立法模式有哪些？我国是使用哪种立法模式？

3. 我国关于“危害计算机信息系统安全罪”的罪名有哪些？

4. 计算机网络作为犯罪目标的刑法规定有哪些？

5.《危害计算机信息系统安全犯罪解释》规范的“六个术语界定”“四个定罪量刑标准”是什么内容？

6. 非法侵入计算机信息系统罪和非法获取计算机信息系统数据、控制计算机信息系统罪（即二百八十五条第一、二款）在侵入行为的入罪方面有何异同？

7. 盗窃虚拟财产犯罪应该如何定罪为宜？

8. 侵入计算机信息系统后，并未破坏计算机信息系统的功能或者数据，而是通过控制计算机实施特定的操作获利的行为是否构成犯罪？

---

① 熊皓、郑兆龙：《如何审查运用电子数据》，载《检察日报》2012年6月5日第3版。

9. 倒卖计算机信息系统控制权的行为如何定罪？

10. 远程控制类程序是否认定为“专门用于侵入、非法控制计算机信息系统的程序、工具”？

11.《刑法修正案(九)》对于“以计算机网络作为工具”实施的传统犯罪是如何规定的？

12. 简述《关于办理网络赌博犯罪案件适用法律若干问题的意见》。

13. 关于淫秽色情的法律法规有哪些？解决了哪些问题？

14.《关于办理网络犯罪案件适用刑事诉讼程序若干问题的意见》(公通字[2014]10号)解决了哪些问题？

15. 电子数据的证据审查规则有哪些？