论非法侵入计算机信息系统罪

赵秉志　于志刚*

一、序　　说

近年来,国外发生的非法侵入计算机信息系统的案件时有报道,危害日益严重。仅在1995年,美国五角大楼的计算机系统就受到25万人的"拜访"。就全世界范围来看,近年较为著名的"侵入"事件有三起,一是1993年英国少年布里顿"侵入"美国国防部计算机系统,接触到了包括弹道武器研究报告、美国情报部门内部机要通讯材料在内的大量机密,并把部分机密输入了有3500万用户的国际计算机网络。第二起是1994年英国电信公司一位计算机操作员"侵入"本公司内部数据库,获得了英国政府防务机构和反间谍机构的电话号码和地址,其中包括英国情报机构、政府的核地下掩体、军事指挥部以及控制中心、英国导弹基地等机密电话号码和梅杰首相的住处以及白金汉宫的私人电话号码。[1] 第三起是美国政府机关遭入侵事件。1996年8月和9月,美国司法部和中央情报局先后遭入侵。入侵者将"美国司法部"的主页改成了"美国不公正部",将司法部长的照片换成了阿道夫·希特勒的照片,将司法部的徽章换成了纳粹党的徽章,并加上一张色情女郎的照片作为司法部长的助手,还在主页上留下了许多攻击美国司法政策的文字。接着,入侵者将中央情报局的主页名称改为"中央愚蠢局",并且同样将主页改得面目全非,最后迫使美国以搜集情报著称的中央情报局关闭了其网络服务器。④ 这是三起令世界震惊的"高技术侵入"事件。而根据美国国防部计算机安全专家对其挂接在INTERNET上的12000台计算机进行的一次安全测试,证明有88%的入侵是成功的,甚至有96%的尝试破坏行为未被发现。随着INTERNET网的迅速扩大,入侵活动也越演越烈,据透露,美国国防部分布很广的全球网络现在平均每天遭到两次袭击。㈣

国际上将上述非法入侵计算机信息系统者称为"黑客"(HACKER),这一词据说源于美国麻省理工学院。当时一个学生组织的一些成员因不满当局对某个计算机系统的使用所采取的限制措施,而开始自己"闲逛"该系统。他们认为任何信息都是公开的,任何人都可以平等地获取。¼ 国内有人将"黑客"称为信息第三者插足,并将其分为突然性信息插足、技术性信息插足、

* 赵秉志,中国人民大学法学院教授;于志刚,中国人民大学法学院博士研究生。

1 参见魏平:《计算机犯罪与计算机战争》,知识出版社1998年版。

④ 参见蔺剑:《各国电脑犯罪与防范新动向》,《国外法制信息》1997年第5期。

㈣ 参见《INTERNET信息安全面临严峻挑战》,《电脑报》1995年12月1日第4版。

¼ 参见黄绍平:《黄与黑——电脑空间犯罪面面观》,《电脑报》1994年4月5日第5版。

欺骗性信息插足和商贸性信息插足等几种情况。[½] 通常情况下在互联网络上的非法侵入者都是那些具有计算机天才的青年学生,这些人可能会整天呆在各种计算机面前试图非法进入某些计算机系统。他们采用各种手段来获得进入计算机系统的口令,闯入系统。他们或者什么都不干就又离开;或者会翻阅感兴趣的资料,进而丰富自己的收藏;更有甚者,可能会攻击系统,使系统部分或者全部崩溃。[¾] 但不可否认的是,目前非法侵入计算机信息系统的行为已经成为窃取计算机内存秘密的最重要方式之一,危害也日趋严重,因而西方各国的刑事立法普遍将其规定为犯罪。

计算机技术的发展和广泛应用是当今信息时代的重要标志。目前在我国,虽然计算机信息系统(网络)的建立和应用与发达国家相比仍有很大差距,但是不得不承认的是,我国的计算机应用已经由单机向联网发展过渡。计算机网络是90年代及未来我国计算机应用发展的重要方向之一,而且在现实生活中,计算机网络的建设和运行近年来也在以惊人的速度发展,地区内、行业系统内乃至全国性的计算机网络纷纷建立,并可通过国际互联网络与世界一百多个国家和地区相联。伴随着计算机网络的逐步联接和广泛应用以及信息高速公路的建立,计算机的安全问题已经成为目前亟待解决的课题,非法侵入计算机信息系统的犯罪也不再是远离我们的事情,其严重的社会危害性已经开始逐步显示出来。鉴于此种行为严重的社会危害性和发展态势,我国修订通过的新刑法典第285条设立了非法侵入计算机信息系统罪,以保护国家各类秘密不受侵犯。

伴随着非法侵入计算机信息系统行为的犯罪化和司法实践中此类案件发案率的逐渐增高,刑法理论界的研究、探讨性文章也日益增多。但应当指出的是,此类犯罪的高技术性导致了对其所进行的刑法学研究必须兼通刑法理论和计算机专业知识,失其一即可能导致论述的浅薄或者定性的偏颇。基于此,我国刑法学界对非法侵入计算机信息系统罪的理论研究尚显苍白。因此,从理论上进一步加深对这一犯罪类型的探讨和研究,对于其正确认定和合理量刑无疑具有重要意义。

二、关于刑法典设立本罪是否必要的争论

尽管非法侵入计算机信息系统的犯罪行为对国家各类秘密造成了严重威胁,具有极为严重的社会危害性,但即使在新刑法典修订通过后,还有论者撰文指出,我国刑法典将非法侵入计算机信息系统的行为单独成罪是毫无意义的。其理由如下:其一,非法侵入可以分为二种,一种是以单纯破译密码为目的的善意侵入,一种是以窃取数据或者程序或者进行其他犯罪的恶意的侵入。前者可能造成骚挠系统的正常运行,但是真正可能造成重大损失的是后者。该论者认为,对于恶意侵入而言,其侵入行为多为深一层的犯罪所吸收,因而法条规定的实际打击对象主要是善意侵入者。但是计算机信息系统不可避免地存在着缺陷,防止和制止恶意侵入的唯一方式是借助于善意侵入者的帮助促进系统的完善。其二,经验表明对于非法侵入行为的查获数量极小,因而法条对无论对善意侵入还是恶意侵入都缺乏有效的威慑作用,只是阻止了善意

½ 参见向荣高:《电脑犯罪与青年》,《中国青年研究》1997年第1期。

¾ 参见梅杰、许榕生:《黑客——游荡在INTERNET上空的又一"幽灵"》,《电脑报》1995年12月9日第4版。

侵入者公布其发现, 使系统丧失了完善的机会, 从而间接地为恶意侵入者开了绿灯。⑧

笔者认为该论者所持的观点是不足取的。不可否认, 非法侵入计算机信息系统的犯罪行为是一种高技术行为, 具有极高的隐蔽性, 犯罪黑数高, 发现率低, 查证率更低。在这一点上, 笔者同意该论者的意见。但应当指出的是, 立法机关之所以将这一类本质在于侵犯国家秘密、科技秘密等秘密的危害行为规定为独立的犯罪, 也正是从这一角度出发的。从实质上或者说从法理上讲, 本罪的犯罪行为, 即非法侵入计算机信息系统的行为, 是一种侵犯各种国家事务秘密、国防秘密和尖端科学技术秘密的犯罪预备行为, 但是由于此类预备行为所涉及的犯罪性质严重, 一旦进一步实施或者实施完毕, 其危害性将变得极为严重, 同时, 此类犯罪即使实施完毕也不一定产生或者说不一定立即产生可以具体确定的实际危害结果, 而且也不一定能够最终被发现、被查证, 因而考虑到这类犯罪严重的社会危害性及其犯罪行为的特殊性质, 我国刑法才将这种实质上的犯罪预备行为法定提前化, 也即把这些预备性质的犯罪行为提升为具体犯罪的犯罪构成中的实行行为, 以严厉打击此类犯罪, 保护各类国家事务秘密、国防秘密和尖端科学技术秘密不受非法侵害。

抛开立法机关规定本罪的立法考虑不讲, 前述论者所持的两个理由也是不能成立的。笔者认为:

其一, 无论是善意的非法侵入行为还是恶意的非法侵入行为, 其行为都是对于国家秘密、国防秘密等的非法侵害, 造成了上述秘密泄露的可能性, 这是非法侵入行为构成犯罪的危害本质所在。对于恶意侵入行为, 尽管其行为可能被后续行为(即该论者所称的深一层犯罪) 所吸收, 但关键在于, 对于深层次犯罪行为的查证率显然要比对非法侵入行为的查证率更低。因而对于立法机关将本罪独立成罪的立法规定方式, 我们无论是将其看作一种实质上的犯罪预备行为, 还是看作一种侵犯各类秘密的危险犯, 都有其立法意义。

其二, 与计算机信息系统的控制访问机制之间的技术对抗, 无论是善意的还是恶意的, 都将有利于系统的改进与完善, 这一点笔者也承认。但是一方面, 我们更应注意的是行为的危害性及其主观罪过。行为有某种程度上的促进作用是一个问题, 而行为本身应受刑罚处罚又是另外一个问题。换一个角度来看, 对他人的某种人身伤害(例如将他人手指用刀砍断) , 可能有助于医疗技术(如外科方面的接骨技术) 的发展, 但却不可能不对伤害行为实施者追究刑事责任。另一方面, 显然不能因为犯罪对象本身的脆弱而放任行为人对犯罪对象的非法侵害, 并借口对犯罪对象有某种促进作用而开脱罪行。

其三, 从技术对抗的角度来分析, 前述论者认为非法侵入行为可以促进系统控制访问机制的完善, 并进而遏制恶意侵入行为。对此笔者也持反对态度。计算机的控制访问机制本身就是对于非法侵入行为的被动反应, 因而仅仅想依靠计算机安全技术的发展和完善来对抗非法侵入的犯罪行为, 不仅是不可能的, 也是不现实的。安全技术与设施是为对抗犯罪行为而出现的, 因而它不仅是后于犯罪行为而出现的, 而且从本质上讲, 它是产生于犯罪行为之中的。从这一角度来讲, 安全技术的开发与使用成本本身就是非法侵入行为所引发的, 这一成本已足以将前述论者称的非法侵入的有利作用全部抵消, 因为无非法侵入行为也就不存在系统的安全机制的存在必要了。再退一步讲, 诚然, 犯罪行为促进技术对抗行为的产生与完善, 但是不可否认, 技术对抗行为反过来又刺激犯罪行为也变成一种更为高级的 "对抗 "技术。如此恶性循环, 使得

⑧ 参见王松江: 《计算机犯罪的概念》, 《法制与社会发展》1997 年第 3 期。

犯罪行为与对抗行为均日趋复杂化。但犯罪行为的复杂化无疑导致犯罪行为更为难以查觉、难以对抗、难以取证, 而正当安全技术(对抗行为) 的复杂化则使其本身更趋于脆弱、更加漏洞百出, 愈发不堪一击。这就是缺乏规范性调整与对抗(包括法律对抗) 的纯科学技术研究与对抗的缺憾。因而, 笔者认为, 从法律上尤其是刑罚上进行主动的规范对抗, 以刑罚的威慑作用来对抗非法侵入的犯罪行为, 无疑是从根本上遏制和打击这一犯罪行为的根本途径。

综上所述, 笔者认为我国刑法将非法侵入特定计算机信息系统的行为独立成罪的立法选择是合理的, 也是必要的。同时也与大多数国家对于此类危害行为的立法规定方式相一致。

三、非法侵入计算机信息系统罪的概念和构成特征

非法侵入计算机信息系统罪, 是指违反国家规定, 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行为。所谓计算机信息系统, 根据 1994 年 2 月 18 日国务院颁布的《信息系统安全保护条例》第 2 条的规定, 是指由计算机及其相关的和配套的设备、设施(含网络) 构成的, 按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

本罪具有如下构成特征:

(一) 犯罪主体特征

本罪的主体是一般主体。凡是达到刑事责任年龄和具备刑事责任能力的人均可构成本罪。在司法实践中本罪的主体一般是具有相当水平的计算机操作人员。这些“侵入者”主要是“计算机玩童”, 他们侵入计算机信息系统往往是出于好奇, 或者为了恶作剧, 有的则为了检验自己的计算机技能。[㈥] 但是, 不可否认的是, 以窃取、非法持有、非法散布各类秘密为目的的非法入侵者在客观上是大量存在的, 而且显然其危害性更为严重。

关于本罪的犯罪主体, 应当注意以下两个问题:

1. 单位是否可以成为本罪的主体

有的学者认为, 单位可以成为本罪的主体。理由是, 修订后的刑法关于计算机犯罪的条款中都加有一个“违反国家规定”前提, 论者认为这里的“规定”主要是指国务院 1991 年颁布的《计算机软件保护条例》和 1994 年颁布实施的《中华人民共和国计算机信息系统保护条例》。而《计算机信息系统保护条例》第 7 条明确规定: “任何组织或者个人, 不得利用计算机信息系统从事危害国家利益、集体利益或者公民合法权益的活动, 不得危害计算机系统的安全。”论者认为这表明单位组织也可以成为计算机犯罪的主体。[㈦]

笔者不赞同这种观点。现行刑法典第 30 条规定: “公司、企业、事业单位、机关、团体实施的危害社会的行为, 法律规定为单位犯罪的, 应当负刑事责任。”根据该条规定, 只有法律明确规定单位可以构成某种犯罪的, 单位才能成为该罪的犯罪主体。而我国现行刑法第 285 条规定的非法侵入特定计算机信息系统罪中, 并未明确规定单位可以成为本罪的主体, 因而应当认为只有自然人才能构成本罪并依法被追究刑事责任。前述论者所依据的《计算机信息系统保护条例》显然不能作为单位也能成为本罪主体的法律依据。虽然该条例规定任何组织也不得实施此

㈥ 参见胡国平: 《关于四种计算机犯罪的认定》, 《法律科学》1997 年第 4 期。

㈦ 参见姚茂文: 《计算机犯罪及实践问题》, 《人民检察》1997 年第 7 期。

类危害行为,但是,该条例在性质上只是国家的一个行政规章,而非可以规定犯罪与刑罚的国家法律,因此违反该条例的行为并非一定被认为是犯罪,进而被追究刑事责任,而仅仅可能被认为是普通的违法行为,仅受到行政处罚或者行政处理。从这个角度上说,单位可能由于实施此类危害行为成为违反行政规章的行为主体,但是却并不能成为非法侵入计算机信息系统罪的犯罪主体。

这里应当指出的是,虽然我国刑法没有将单位规定为非法侵入计算机信息系统罪的主体,但是对于本罪而言,单位犯罪在计算机普及程度将来有极大提高后肯定会大量出现,这一点在西方发达国家的立法中已有反映。我国目前计算机普及程度较低,在目前已经发生的非法侵入计算机系统的犯罪案件中,个人犯罪占绝对多数,同时我国的计算机犯罪尚处于简单犯罪阶段,因而刑法未将单位规定为本罪的犯罪主体是符合我国目前此类犯罪的现状的。但是,单位犯罪的出现和刑法将单位收纳为本罪的主体在本罪的实际发展和法律惩治过程中都同样是不可避免的。值得一提的是,国外已存在惩治单位实施此类犯罪的立法例。[10]

2. 境外人员实施此类危害行为的刑事责任

计算机网络从某种意义上消除了社会和空间界限,消除了国境线,但由此引发的一个问题是,实施各类计算机空间犯罪的人的空间位置也同时超越了国境线。通过国际互联网络实施犯罪行为的人数猛增,跨国界犯罪在所有计算机犯罪中所占的比例越来越高。近年来较为典型的一个跨国界的计算机犯罪的案例是几名联邦德国学生通过国际互联网络进入美国国防部为克格勃窃取军事机密一案。这几名学生先从西德登陆到日本,然后从日本登陆到美国的一所大学,再从这所大学登陆到美国国防部的军用计算机信息系统并进而窃取军事秘密。[11] 对于此种跨国境的非法侵入计算机信息系统的案件,如果所侵入的计算机信息系统是在我国境内,则显然应当适用我国刑法,依法追究非法入侵者的刑事责任。对此我国刑法学界没有异议。

有的学者认为,对于此类行为人处于我国境外,通过互联网络实施的非法侵入我国国家事务、国防建设、尖端科学技术领域的计算机信息系统的行为,适用我国刑法的根据是刑法总则第 8 条,即:“外国人在中华人民共和国领域外对中华人民共和国国家或者公民犯罪,而按本法规定的最低刑为 3 年有期徒刑的,可以适用本法,但是按照犯罪地的法律不受处罚的除外。”[12] 但是有的学者持不同意见,认为适用我国刑法的根据是刑法总则规定的第 6 条第 3 款,即:“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。”[13]

笔者赞同后一种观点,因为此类跨国境犯罪的犯罪行为虽然不在我国境内实施,但是犯罪结果显然是发生在我国领域内的,因而显然符合该条的规定。而前一种观点的不妥之处有两点:一是我国刑法第 8 条所规定的外国人在我国领域外犯罪适用我国刑法的保护主义管辖规定,是特别针对犯罪主体不是中国人,同是犯罪不发生在我国领域内的犯罪而言,只有在这种情况下才能适用该条的规定,而对于犯罪行为或者结果有一项发生在我国领域内的犯罪,则应当视为 在我国领域内犯罪,从而不应当适用该条。二是该论者一方面强调此类犯罪行为应当依照我国刑法追究刑事责任,另一方面又坚持应当依照刑法第 8 条的规定适用我国刑罚,这无

10 参见《德国刑法典》第 323—6 条,罗结珍译,中国人民公安大学出版社 1995 年版,第 128 页。
11 参见前引[4],梅杰等文。
12 前引[7],姚茂文文。
13 参见姚青林:《论侵入重要领域计算机信息系统罪》,《人民检察》1997 年第 8 期。

疑有前后自我矛盾之处。因为根据该条的规定,外国人在我国领域外对我国国家或者公民犯罪,只有该犯罪的法定最低刑为3年以上有期徒刑的,才适用我国刑法。但是对于本罪而言,根据刑法第285条的规定,本罪的法定刑为3年以下有期徒刑或者拘役,因而如果依照该论者的观点,对于外国人在我国领域外实施非法侵入我国国内的特定计算机信息系统这一犯罪行为的,我国刑法无管辖权。这不但是该论者前后观点的自相矛盾,而且对于维护我国国家主权和国家权益是极为不利的,也是极为不妥的。

非法侵入计算机信息系统罪是一种新型的犯罪,同其他刑事犯罪相比具有较多的不同之处。而此种犯罪类型中,外国人在我国领域外通过国际互联网络侵入我国境内的特定计算机信息系统的犯罪行为则更具有特殊性。尽管我国1979年刑法就有"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"的规定,但是众所周知,在司法实践中,犯罪行为或者结果不同时发生在中华人民共和国领域内的犯罪是极为少见的,外国人在我国领域外对我国领域内的犯罪对象犯罪更是少之又少。有的刑法教科书所举的案例,例如在国境外开枪,打死了境内的人员,在司法实践中也是不太可能发生的,即使发生了也较为少见。但正是由于此类犯罪的数量较少,也使得这对极少数犯罪适用我国刑法显得不太脱离实际。但是非法侵入计算机信息系统的犯罪却不同,因为在计算机网络空间上是没有领土边界的,在网络逐渐普及的将来,此类犯罪行为可能会大量发生,对于此种犯罪行为处于领域外而犯罪结果发生于领域内的犯罪,我们对实施犯罪行为的外国人追究刑事责任比以前更为困难,这不仅是刑事管辖权的具体实施问题,而且还因为"把任何给定的信息从A点传输到B点要牵涉成千上万的计算机和许多不同的环节,因此,按照法庭诉讼的可靠性证明它实际上是从A点出发并且的确到达B点可能是极为困难的。"[14] 对于此种情况,如前所述,直接适用我国刑法的地域管辖权是可行的,但是管辖方式并不限于此,例如英国的《滥用计算机法》就规定:只要被侵入的计算机在英国,该法就适用,而不论行为实施者在何处。我们认为这种立法方式是可资借鉴的。

(二)犯罪主观特征

本罪的主观方面是故意,即明知是特定的计算机信息系统而仍然故意实施侵入行为。至于行为人的动机则可能是多种多样的,如出于好奇、追求刺激、显示个人技能等。例如,美国空军的一个网站于1997年的某一天被非法入侵,并被帖上色情图片、猥亵与反政府文字,声称自己是一位23岁的圣地亚哥男子表示,这件事是他们干的。他表示,其目的仅仅是要告诉美国空军的网站一定要提升保护措施,因为所有政府单位的计算机安全防范措施实在太脆弱了!根本阻止不了任何人。因为他们之中的一人只有15岁。他认为,外国政府在几分钟之内就可以突破这样的安全措施。[15]

对于非法侵入计算机信息系统罪的主观方面,应当注意以下两个方面的问题:

1. 犯罪目的

正如有的学者所言,破坏安全系统进而实施的犯罪行为可能涉及对隐私权的侵害、商业秘密的侵害或者知识产权的侵害,因而与侵入行为本身对安全系统的破坏形成了方法与结果行为的牵连关系。[16] 因而应当注意的是,如果行为人具有其他特定的犯罪目而实施非法侵入计算

14 参见前引⑦,姚茂文文;前引13,姚青林文。

15 参见张明伟:《美国空军网站遭入侵》,《电脑报》1997年1月17日。

16 参见[美]刘江彬:《计算机法律概论》,北京大学出版社1992年版,第157页。

机信息系统的, 如以非法获取国家秘密、商业秘密等为目的, 则存在方法行为与结果行为或者说目的行为与手段行为的牵连关系, 因而应当从一重论处。笔者以为, 通常应当以其目的行为所构成的具体犯罪追究刑事责任, 如非法获取国家秘密罪、侵犯商业秘密罪或者以某种特定危害国家安全罪追究刑事责任更为妥当一些。而且由于本罪规定的法定刑过低, 即使按照从一重处罚的原则, 也往往不以本罪追究犯罪人的刑事责任。

从另一个角度讲, 本罪行为人主观方面的目的和非法持有毒品罪的主观方面的目的具有相似性。即非法侵入的犯罪目的应当具有某种程度上的潜在的多样性和当前目的的不可查证性。[17] 对于非法持有毒品罪的犯罪目的而言, 由于该法条规定的特殊性和持有行为本身所处阶段的特殊性, 因而其犯罪目的如果能够查证为出于走私、贩卖、运输、制造或者窝藏的目的, 则已超出非法持有毒品罪所能容纳的范畴, 而应当以其犯罪目的所构成的具体犯罪定罪量刑。对于本罪而言, 如果能够查明是出于其他犯罪目的而非法侵入计算机信息系统的, 则要么非法侵入行为被其他犯罪行为所吸收, 不再以本罪进行处罚, 而可能以其他犯罪追究刑事责任, 如间谍罪等; 要么非法侵入行为和其目的行为构成牵连关系, 应当从一重论处。

事实上, 非法侵入计算机信息系统是对计算机信息系统安全体系的破坏, 而这种破坏是一个较为广泛的概念, 它往往被更深入一层的犯罪行为所吸收, 因此犯罪独立存在的情况是比较少见的。[18]

2. 过失能否构成本罪

有学者认为过失也可构成本罪。理由是: 为了从法律上保护国家计算机信息系统不受侵害, 特别是考虑到计算机系统被破坏后将造成的重大损失, 对过失犯罪也应当定罪处罚。并认为由于计算机犯罪主观认定的复杂性, 如果不设立过失犯罪, 任何人都可将自己侵入计算机系统的行为表白为疏忽大意所致, 其结果将导致保护不力[19]。

笔者不赞同这种观点。众所周知, 我国刑法以处罚故意犯罪为原则, 以处罚过失犯罪为例外, 因而现行刑法第 15 条第 2 款规定: "过失犯罪, 法律有规定的才负刑事责任。"这一规定意味着, 对于某一犯罪行为, 只有当 法律明确规定处罚其过失犯罪的, 才能对过失犯该罪的行为追究刑事责任。而由于现行刑法未规定过失行为可以构成非法侵入特定计算机信息系统罪, 因此本罪的主观方面只能是故意而不可能是过失。另外, 从实践中发生的案例来看, 非法侵入行为一般情况下也只能是故意, 因为各类计算机信息系统一般均有特殊的控制访问机制也即安全保卫机制, 这对于作为本罪犯罪对象的国家事务、国防建设、尖端科学技术领域的计算机信息系统而言更是如此, 因此行为人如果不作技术等方面的努力一般是不可能破译密码而突破此类安全保卫机制或者成功绕过此类安全保卫机制的, 纯过失而误入此类计算机信息系统的行为是不存在的。

基于以上理由, 笔者不同意下述观点: 有的学者指出, "过失侵入国家重要领域计算机信息系统, 不构成该罪。但如果是过失侵犯而退出的仍可构成该罪, 法国刑法典就有类似规定。"[20] 笔者以为, 首先, 根据以上理由, 纯过失地侵入国家重要计算机信息系统的行为是不存在的, 因而也不存在过失侵入而不构成犯罪的情况及对此种情况探讨的必要性; 其次, 该论者的观点似

17 参见于志刚: 《毒品犯罪之理论问题研究》, 时事出版社 1997 年版, 第 254 页。
18 参见前引16 , 刘江彬书。
19 参见前引㊦, 姚茂文文。
20 前引13 , 姚青林文。

乎存在自相矛盾之处。何谓过失侵入而不构成犯罪,过失侵入而退出仍可构成犯罪呢?另外,笔者仔细翻阅了法国刑法典,也未找到论者所称的过失侵入而后退出的仍可构成犯罪的法条规定。

(三)犯罪客观特征

本罪客观方面表现为违反国家规定,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行为。

准确把握本罪的客观特征,应当从以下几个方面入手:

1. "侵入"一词的含义

所谓"侵入",是指非法用户调取、访问计算机信息系统内的系统资源的行为。一般而言,所有的计算机信息系统都有其自身的安全控制机制,这一机制可以鉴别并给用户以访问授权,也就是说它可以决定哪些用户有访问计算机信息系统的权力,并在此基础上明确规定合法用户的访问权限。计算机信息系统的安全机制分为二类:一是对用户进行常规识别,以确定用户的身份,从而防止非法入侵者入侵系统;二是系统内部用户对系统资源的访问控制,也即对合法用户的访问权限进行限制,一般而言,在某一信息系统内极少有某一合法用户对系统内部资源拥有不受限制的访问权限,这在重要的计算机信息系统内更是如此。

根据上述用户的身份特征和访问权限来划分,非法侵入行为的非法性可以分为两类:一是非法用户侵入信息系统,也即无权访问特定信息系统的人非法侵入该信息系统。二是合法用户的越权访问,也即有权访问特定信息系统的用户,未经批准、授权或者未办理手续而擅自访问该信息系统或者调取系统内部资源。在现实生活中发生的非法入侵行为主要是指前者,而且一般认为我国刑法所打击的非法入侵行为也主要是指前者。

有的学者根据侵入行为的实施者在侵入后是否有进一步的犯罪行为(如窃密等——笔者注),而将侵入分为善意侵入和恶意侵入两种。[21] 笔者不赞同这种观点,认为对于本罪的侵入行为,法条规定了"违反国家规定"一词及"侵"字的含义,已表明了行为人的主观罪过,因而从未经授权这一角度来衡量,所有的侵入行为可以说均是"恶意"的,而无善意的可能。同时,以是否实施更为严重的犯罪行为作为标准,将犯罪人的主观罪过界定为"善"与"恶",也与法理不符。

2. "非法"的应有之义

对于本罪的客观行为而言,应当提出的是,行为人通过各种手段进入上述特定计算机信息系统的行为是违反国家规定的,也即是未经合法授权的"非法"入侵行为。

对于"非法"一词,新刑法典规定本罪的法律条文也即第285条未明确规定,但是刑法理论界和司法实践部门无一例外地将本罪的罪名贯之以"非法侵入计算机信息系统罪",最高司法机关有关罪名的解释也持同样看法。[22] 因而我们这里必须对于"非法"含义进行合理的探讨。

对于"非法"的确切含义,应当从有关立法机关和司法机关的法律文件中来探根溯源。关于非法侵入计算机信息系统罪的立法文件,最早见于全国人民代表大会法律工作委员会1996年10月10日印行的,《中华人民共和国刑法(修订草案)》(征求意见稿)的第254条,该条规定:"违反规定,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3年以下有

21 参见前引⑧,王松江文。

22 参见最高人民法院审判委员会第951次通过的《关于〈中华人民共和国刑法〉罪名的规定》。

期徒刑或者拘役, 可以并处或者单处罚金。"[23] 除了 1996 年 12 月 20 日的《中华人民共和国刑法(修订草案)》第 259 条将"违反规定"修改为"违反国家规定"以外,[24] 其他的历次草案(指 1997 年 2 月 17 日及 1997 年 3 月 1 日的《中华人民共和国刑法(修订草案)》)对于本罪均是法定刑罚幅度或者刑种上的变动, 而未再作实质性修改。而对于本罪立法过程中的更早源头, 则可溯及至公安部修改刑法领导小组办公室 1996 年 8 月《危害计算机信息系统安全罪方案》(公安部修改刑法研究方案之八,[25] 该方案第 1 条规定了非法进入计算机信息系统罪, 内容为"未经许可, 擅自进入国家事务、经济建设、国防建设、尖端科学技术领域的计算机信息系统的, 处 5 年以下有期徒刑、拘役, 可以单处或者并处罚金。"从以上对比可以看出,"非法"的最初含义是"未经许可, 擅自进入", 而后发展演变为"违反规定"、"违反国家规定", 其范围和所违反对象本身是在不断一步步缩小的, 由违反客体不明的"未经许可", 最终缩小到"违反国家规定"。而对于"国家规定"的具体范围, 新刑法典第 96 条则作了明确规定。结合新刑法该条和第 285 条的规定, 我们认为这里的"非法"应当是指第 285 条所称的"违反国家规定", 而所谓违反国家规定, 具体到本罪而言, 是指违背国家关于计算机信息系统管理的各项法律、法规, 不具有合法身份或者条件而未经授权的擅自侵入。例如违反前述的《计算机信息系统安全保护条例》。目前我国关于计算机信息系统管理方面的法规还有《计算机信息网络国际联网管理暂行规定》、《计算机信息网络国际联网出入信道管理办法》、《中国公用计算机互联网国际联网管理办法》、《专用网与公用网联网的暂行规定》等, 违反上述规定、办法均可视为违反国家规定。

3. 侵入的对象与方式

对于本罪而言, 必须具有"非法侵入"行为, 而且非法侵入的是国家事务、国防建设和尖端科学技术领域的计算机信息系统。

如前所述, 从用户的身份特征和访问权限来看, 非法侵入行为的非法性可以分为非法用户侵入信息系统和合法用户的越权访问。

通常情况下非法用户的侵入方式可以分为以下几种:

其一, 冒充合法用户。也即不具有合法用户身份者冒充合法用户而进入计算机信息系统。常见的冒充的方式有以下几种: 一是使用别人的访问代码冒充合法用户进入计算机信息系统, 而无论其所使用的他人的访问代码是偷窃来的, 还是以其他非法方式获得的(如通过设立陷阱程序骗取合法用户的代码等)。对于此种情况, 有的学者指出, 此种行为经常发生牵连犯罪的情况, 比如行为人所窃取的口令是国家绝密材料, 则构成了窃取国家秘密罪, 因而其手段行为触犯一罪, 而目的行为又触犯另一罪, 因而构成牵连犯。[26] 笔者赞成这种观点。二是"乘机而入", 即"侵入者"利用合法用户输入口令(password)之机获取访问(access), 或合法用户结束使用但未退出联机之前获得访问的一种方法。这就像小偷正要撬门而有人进出就乘机混入大门一样。三是利用非法程序或方法蒙骗正在向计算机登录的合法用户以进入系统。比如, 利用寄生术(piggyback)。寄生术是指跟随其他用户的合法访问操作混入计算机系统作案的一种方法。[27]

23 参见赵秉志主编:《新刑法全书》, 中国人民公安大学出版社 1997 年版, 第 1755 页。
24 前引[23], 赵秉志主编书, 第 1781 页。
25 转引自高铭暄、赵秉志编:《新中国刑事立法资料总览》, 中国人民公安大学出版社 1997 年版。
26 前引[13], 姚青林文。
27 参见前引[七], 胡国平文。

其二,采用计算机技术进行技术攻击。也就是说,非法用户针对前述所讲的计算机信息系统的身份识别机制采用计算机技术进行攻击,以图达到绕过或突破此类硬件及软件访问、存取控制机制以进入系统。技术攻击的方法从总的来说有两种,一是技术突破,即通过猜想口令等方法硬性闯过安全防卫机制;二是绕过,即避开安全防卫机制进入计算机信息系统。在这一点上,此种方式和第二次世界大战中德军绕过法国的"马其诺"防线较为相似。当时法国为了防止德军从德法边境入侵而修建了长达数百公里,宽约数十公里的"马其诺"防线,但是法国人忘记了法国的边境除了法德边境外还有法荷边境,结果德军从法荷边境长驱直入而进入法国,使"马其诺"防线失去了作用。而在计算机信息系统的安全防卫机制中,同样存在众多可以绕过的地方,因而往往使经过精心设计的安全控制机制归于无效。

目前实践中为防止非法用户的入侵而采取的用户身份识别机制或者措施主要有以下几种:一是基于用户独具知识的身份识别,如用户的ID号码、口令、密钥等;二是基于用户物理特征的身份识别,如声音、像貌、指纹、签字等;三是基于用户所持证件的身份识别,如光卡、磁卡等;四是基于上述各种方法的组合而采取的身份识别。[28] 这些身份识别措施可以归纳为二类:一是利用生物学方法寻求用户个人的唯一识别信息,如指纹、手纹、唇纹等,这些特征是与用户个人紧密相关而且通常情况下是唯一的,因而较难仿冒。但是缺点是占用内存容量大,运行不太准确,因而在现阶段难以大规模进行推广。二是利用密码理论和密码技术通过确定用户代号来达到身份识别的目的。这是现实中较为常用的一种方法。通常是采用输入用户识别号(如ID号码)和输入一个由用户自己记忆的不常变化的口令(PW)的办法。但是ID号码是公开的,而口令则通常字符较短,极容易被破译。事实上,密码代号的识别防范机制在某种程度上会极大刺激非法侵入行为的增长,就现实中相当大一部分非法侵入计算机信息系统的案件的行为人而言,其犯罪动机仅仅在于通过破译密码、侵入防范严密的特定计算机信息系统来显示其个人的聪明才智。

实践中常见的以直接采用计算机技术攻击方式非法侵入计算机信息系统的行为方式主要有以下几种:一是利用网络设计缺陷,比如在INTERNET(全球计算机网络)中,一种被称为"路线标定者"的特殊网络由计算机决定信息数据的确认和配送。非法侵入者则利用网络设计上的一个缺陷,采用欺骗"路线标定者"的办法冒充合法用户,从而得到受保护的计算机数据资源通道,控制了有关系统。二是搜索系统口令表,也就是入侵者通过访问并修改系统口令表,设假口令从而达到非法侵入的目的。三是直接破译用户身份识别密码或者口令。这是最为常见的攻击方法,也最容易得逞。四是开发欺骗程序。例如有关国家曾经开发出一种全新的计算机信息系统安全防卫形式——电话回拨系统,也就是说,合法用户访问这种系统时要输入自己的ID号(用户身份号)和口令字,系统据此查出用户的电话号码,并挂断用户拨入的电话,然后回拨给用户,据此识别和证明用户的合法身份。但是,一些不法之徒"开发"出了一些能使电话回拨系统失去作用的程序,通过电话进入电话回拨系统,使回拨系统不能真正挂断电话,当系统回拨后模仿其拨号声,让电话一直接通而直接闯入信息系统。[29] 最新的非法入侵手段是于1994年12月5日才被首次发现的"INTERNET规程欺骗"。这种方法是给路由器造成一个可靠发信人正在试图向收信人发送信息的假象,在得到认可后进入到作为目标的计算机信息系统内。

28 参见前引13,姚青林文。

29 参见《INTERNET信息安全面临严峻挑战》,《电脑报》1995年12月1日第4版。

1994 年 12 月 5 日, 一位在美国圣地亚哥巨型机中心工作的著名计算机安全专家的机器遭到入侵, 不知不觉被占用了一天多时间, 该专家为保护计算机安全而设计的大量软件被盗走, 这才使得“INTERNET 规程欺骗”方法被发现。[30]

其三, 通过“后门”进行非法入侵。“后门”一般是由软件作者出于维护或其他理由而设置的一个隐藏或伪装的程序或系统的一个入口。例如, 一个操作系统的口令机构可能隐含这样一个后门, 它可以使一定序列的控制字符允许访问经理的帐号。当一个后门被人发现以后, 就可能被未授权用户恶意使用。

其四, 通过“陷阱门”进行非法入侵。陷阱门也叫活门。在计算机技术中, 是指为了调试程序或处理计算机内部意外事件而预先设计的自动转移条件。陷阱一般只有制造商知道, 不告诉用户。程序调好后应关闭陷阱。如果厂商交货时忘记关闭陷阱, 就会被人利用而绕过保护机制, 然后进入系统。[31] 非法侵入计算机信息系统的第二种情况是合法用户的越权访问。一般情况下, 某一计算机信息系统的合法用户是有权访问该信息系统或者调取其内部资源的。但是, 合法用户的访问权是有限制的, 换言之, 其访问权一般只限于访问该信息系统的某些部分, 或者只能调取该信息系统内部资源信息的某些部分。访问权的大小和级别通常根据用户的身份、地位、工作需要而决定, 极少有不受任何限制的用户访问权, 这对于国家事务、国防建设、尖端科学技术领域等重要计算机信息系统来说更是如此。

系统内部的访问控制机制目前主要有两种, 一种是自主控制访问机制, 就是用户可以随意在系统中定义谁可以访问他们的文件; 一种是强制访问控制机制, 在此种机制中, 用户和文件都有固定的安全属性, 这些属性由系统使用, 以决定某个用户是否可以访问某个文件。[32] 强制访问控制机制是比任意访问控制机制更强的一种控制访问机制, 这可以通过无法回避的访问限制来防止某些对系统的非法入侵。在强制访问控制机制下, 安全属性是由系统自动地或者由系统管理员或者系统安全员人工分配给每一个主体或者内部资源文件的。这些属性不能被任意更改。它通过比较访问者和被访问资源文件的安全属性来决定是否允许用户调取系统内部资源文件, 如果系统认为具有某一安全属性的访问者不能访问具有一定安全属性的资源文件, 那么任何人都无法使该访问者接触到该资源文件。代表用户的应用程序不能改变自身的或者其他资源文件的安全属性, 也不能把某一文件的访问权授予其他用户。而自主访问控制机制则不能有效对抗非法入侵者的渗透入侵, 例如“特洛伊木马”程序这种技术渗透。因为在自主访问控制中, 某一合法用户可以任意运行一段程序来修改该用户拥有的文件的访问控制信息, 而操作系统无法区别这种修改是用户自己的非法操作还是“特洛伊木马”的非法操作。强制访问控制机制通常和自主访问控制机制相结合使用, 以确保用户只有在通过了自主与强制访问机制检查后, 才能访问某个系统或者其内部资源文件, 从而防止非法者入侵或者合法用户的越权访问。

合法用户只能在其所拥有的访问权限以内行使访问权, 任何未经批准、授权的越级、越权访问或者调取, 均属于非法侵入, 而无论其采用何种侵入方法。从实质上讲, 这种非法侵入同上述非法用户的非法侵入在性质上是相同的。也就是说, 只要合法用户越权侵入系统, 其身份即由合法变为非法。换言之, 合法用户也可以通过或者借助计算机技术或者外界帮助以突破内部

30 同上注。
31 参见前引(七), 胡国平文。
32 参见李海泉编著: 《计算机系统安全技术与方法》, 西安电子科技大学出版社 1997 年版。

的访问控制机制, 从而实现对信息系统的侵入, 也可以通过借助隐蔽通道进入系统。

非法侵入计算机信息系统的方式从与计算机信息系统的距离远近来看, 可以分为直接侵入和间接侵入两种方式。直接侵入又可分为接触式侵入和本地侵入两种方式。前者是指直接运用前述三类计算机信息系统的某个终端实现直接操作; 后者是指运用上述三种计算机信息系统专用设备实现联机侵入。间接侵入可以有广域网侵入和局域网侵入。前者是指远途侵入, 一般是采用电话线进行登录, 后者则一般是使用专用计算机光缆侵入。[33]

4. 侵入行为的未遂与既遂

有的学者认为, 本罪是行为犯, 只要查证行为人有侵入信息系统的事实, 即构成犯罪既遂。[34] 有的学者持相似观点, 并同时进一步指出, 本罪的既遂并不要求将行为人侵入信息系统行为产生的后果作为成立犯罪的必备要件。持此论者认为, 本罪的犯罪形态只存在犯罪预备、犯罪中止和犯罪既遂三种形态而没有犯罪未遂形态, 而判断犯罪预备与犯罪既遂界限的标准应当是行为人的入侵行为是否已突破或者绕过系统的安全机制。[35]

笔者不赞成这种观点。尽管对于本罪而言, 只要行为人有非法侵入特定计算机信息系统的行为即可构成犯罪, 而对行为人非法入侵特定计算机信息系统后是否实施其他行为或者是否造成其他后果并无特殊要求, 但这并不足以说明本罪是行为犯, 更不能由此判断本罪不存在犯罪未遂。非法侵入特定计算机信息系统的行为是一个完整的行为, 可能停止在任何未完成形态。如试图非法侵入国防建设的计算机信息系统而多次尝试攻击, 但由于个人技术的欠缺而均告失败的, 显然属于犯罪未遂。事实上, 实践中所发生的绝大多数试图入侵行为均是未成功的, 成功入侵的行为据统计只占全部攻击次数的 15% 左右。

但是应当指出的是, 上述论者所提出的判断犯罪预备与犯罪既遂的界限标准, 如果作为判断犯罪既遂与否的标准则是可取的, 也即犯罪既遂与否的界限标准应当以行为人的入侵行为是否已突破或者绕过系统的安全保卫机制来进行判断。换言之, 应当把握住本罪中犯罪行为的本质特征来考察犯罪行为的既遂与未遂问题。本罪的犯罪方法依法条表述为 "侵入 ", 因而顾名思义, 已经 "侵入 "计算机信息系统的, 应当视为犯罪既遂; 而 "侵而未入 "的, 则显然应当认为是犯罪未遂。

(四) 犯罪客体特征

本罪所侵犯的客体是国家重要领域计算机信息系统的安全。

随着计算机在我国的日益普及化, 各种国家事务秘密、国防建设秘密以及尖端科学技术秘密越来越多地保存在计算机信息系统中或者说以计算机存储数据的方式出现。因而计算机信息系统的安全对于国家重要部门和重要事务的影响越来越大, 保证这些重要部门的计算机信息系统的安全, 对于保护各种国家秘密、国防秘密、尖端科学技术秘密不受侵犯, 对于维护正常的社会秩序和保卫国家安全, 无疑起着重要的作用。

如前所述, 在现实生活中固然有一部分非法侵入的犯罪行为, 其目的是为显示超群才智, 以单纯破解安全密码为目的, 换言之, 其目的是单纯的非法侵入计算机信息系统内部, 以显示安全控制机制对其并不起任何阻碍作用, 而并不是针对计算机信息系统内部所存储的数据和秘密的, 似乎并未造成实质上的重大损害。但是事实并非如此, 这正如有的学者所言, 一个被侵

33 参见于志刚: 《新刑法典拆解比较与适用》, 中国经济出版社 1997 年版, 第 755 页。
34 参见前引(七), 胡国平文。
35 参见前引13 , 姚青林文。

入的计算机中心, 其心理及精神上的损失是无法估计的, 被侵入的安全系统势必重新布置, 严加防范, 时间上和精力上的花费都很大。[36]

本罪的犯罪对象是特定计算机信息系统。所谓计算机信息系统, 如前所述, 是指由计算机及其相关的和配套的设备、设施(含网络) 构成的, 按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

但是应当注意的是, 并非所有的计算机信息系统均可成为本罪的犯罪对象, 具体而言, 本罪的犯罪对象仅限于国家事务、国防建设、尖端科学技术领域的计算机信息系统, 因而非法侵入其他计算机信息系统的, 不构成本罪, 但是可能构成其他犯罪。计算机信息系统的外延是非常广泛的, 其表现形式也多种多样。按照系统内计算机组成构成来划分, 可将计算机信息系统分为两类, 一类是只包括一台计算机系统的信息系统, 另一类是由多个计算机系统组成的分布式系统。无论哪一种系统都可以成为国家事务、国防建设和尖端科学技术领域的计算机信息系统。确定哪一个系统属于国家事务、国防建设和尖端科学技术领域的计算机信息系统, 有的学者指出, 主要是看该系统所采集、加工、存储、传输、检索的信息属于何种性质, 具体的技术性规定应由国家相关部门发布规章加以规定。[37] 笔者同意这种观点, 但认为应当进一步深化, 即何谓此三类计算机信息系统, 不仅要以其内部存储信息的性质作为判断标准, 而且要和保守国家秘密的有关法规相连起来进行判断。

四、非法侵入计算机信息系统的后续行为的认定

如前所述, 非法侵入计算机信息系统的犯罪行为不以行为人侵入计算机信息系统后产生的后果作为构成要件, 只要行为人实施了非法侵入计算机信息系统的行为即可构成犯罪。对此我国刑法学界没有异议。但是, 单纯出于破解密码、突破安全控制访问机制、以显示个人超凡才智为动机的非法入侵行为只是所有非法入侵行为的一部分。而且, 即使对这部分非法侵入行为来说, 侵入后什么也不干即自行离开的事情也是极为少见的。从另一个角度来讲, 非法侵入计算机信息系统的行为通常伴随着某种后续性行为, 当然此种后续性行为可能与计算机信息系统安全控制访问机制所保护的核心内容有关系, 也可能没有关系。恶作剧式的侵入(并不涉及内部秘密的侵入) 后即自行退出的行为也是存在的, 例如著名的美国司法部网络系统被入侵案。但即使对于此类案件而言, 也应当以非法侵入计算机信息系统罪追究刑事责任。惩罚此类入侵行为的关键之处在于, 其非法入侵计算机信息系统的行为已经使国家事务秘密、国防建设秘密和尖端科学技术秘密等受保护的秘密超出了限定的受权接触范围, 并且行为人不能证明上述秘密未被不能知悉的人(包括入侵者本人和其他人) 知悉。对于 此种以保护秘密为目的而设立的特殊处罚和求证原则, 我国有关法律也已有类似规定。[38]

对于实施后续性行为的处理, 通常情况下应当具体情况具体对待, 依照以下原则处理: (1) 非法侵入计算机信息系统后窃取各种国家事务秘密、国防建设秘密和尖端科学技术秘密的, 如果出于好奇的目的而非法获取的, 应当以非法获取国家秘密罪和非法侵入计算机信息系统罪

36 参见前引16 , 刘江彬书。

37 参见前引13 , 姚青林文。

38 参见《中华人民共和国保守国家秘密法实施办法》第 35 条, 1990 年 5 月 25 日国家保密局令第 1 号, 转引自《中华人民共和国常用法律大全》, 法律出版社 1996 年版, 第 719 页。

实行数罪并罚。(2) 非法侵入计算机信息系统后对于计算机信息系统的功能进行删除、修改、增加、干扰, 造成计算机信息系统后不能正常运行, 后果严重的, 应当以非法侵入计算机信息系统罪和破坏计算机信息系统功能罪实行数罪并罚。(3) 非法侵入计算机信息系统后对于计算机信息系统存储、处理、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, 应当以非法侵入计算机信息系统罪和破坏计算机信息系统数据和应用程序罪实行数罪并罚。

对于以上几种非法侵入计算机信息系统后的后续性行为而言, 其应当共同注意的是牵连犯问题。基本的处理方式是, 在非法侵入之前已经有侵入后实行某一犯罪行为的犯罪目的, 如以为境外窃取、刺探计算机信息系统内部存储的国家事务秘密、国防建设秘密和尖端科学技术秘密等为目的而实施非法侵入行为的, 构成牵连犯, 应当从重处罚。而如果行为人后续行为的犯罪是在非法侵入计算机信息系统后才产生并付诸于实践的, 则应当以非法侵入计算机信息系统罪和后续行为所构成的犯罪实行数罪并罚。例如美国少年米尼克, 1979 年运用破译计算机安全密码的特殊才能, 成功地打入 "北美防空指挥中心电脑系统 "后, 将美国瞄准前苏联的核弹头绝密资料一览无疑。[39] 对于此案, 如果尼米克在展示自己的才能, 侵入后自行离去, 依照我国刑法典来衡量, 则仅应当以非法侵入计算机信息系统罪来处罚即可; 但其侵入后又临时起意而非法获取军事绝密材料, 则应当两罪进行数罪并罚。

五、非法侵入计算机信息系统罪的处罚

根据现行刑法第 285 条的规定, 犯非法侵入特定计算机信息系统罪的, 处 3 年以下有期徒刑或者拘役。

对于非法侵入计算机信息系统罪的刑罚适用, 笔者认为应当考虑以下两个方面的因素:

1. 所侵入的计算机信息系统的重要性

如前所述, 对于非法侵入计算机信息系统行为的单独设立一罪, 是为加强对危害国家事务秘密、国防建设秘密和尖端科学技术秘密的法定保护, 避免此类秘密的泄露。因而对于非法侵入计算机信息系统的行为适用刑罚的一个重要原则, 是考虑非法侵入的计算机信息系统的属性及其重要程度。换言之, 应当着重考虑所被侵入的计算机信息系统的重要程度, 而这种重要程度应当和该计算机信息系统所属单位的属性有直接联系。进一步讲, 侵入关系到国家重大决策、国防布署等极重要计算机信息系统的, 应当处以法定刑罚幅度内较重的刑罚; 侵入一般的国家事务、国防建设等计算机信息系统的, 应当在法定刑罚幅度内处以较轻的刑罚。

2. 其他情节因素

具体而言, 影响本罪刑罚适用的可能有以下情节: 非法侵入前述三类计算机信息系统的次数、范围; 所造成的实际影响程度; 是否有已经构成其他犯罪的后续性行为等。具有以上所述情节的, 应当在法定刑罚幅度内适用较重的法定刑; 没有上述情节, 仅仅是非法侵入后即自行离开的, 可以在法定刑罚内适用较轻的刑罚。

39 参见赵廷光: 《信息时代、电脑犯罪与刑事立法》, 载《刑法修改建议文集》(高铭暄主编), 中国人民大学出版社 1997 年版。