使用大字体察看本文
阅读次数：1406

网络犯罪停止形态

丁英华

随着信息网络的逐渐普及，新型网络犯罪不断涌现，并且逐渐波及至传统犯罪，出现了传统犯罪网络化的趋势。其中大多数犯罪在刑法中理论中已有明确具体的规定与解决办法，所不同的是犯罪手段犯罪形式上有所改变，采用计算机，网络技术手段实施的犯罪行为，虽然其形式外观上是新的，但并没有产生新的法律问题，在现有刑法体系内仍可以得到解决，不会发生适用上的困难。有些犯罪则超出了现行刑事法律的范围，司法实践中对这类犯罪适用刑法存在一定困难。因此研究网络犯罪，应该将这些新型的犯罪作为研究的重点，有针对性的加以剖析。本文试从我国新刑法中新增的若干种网络犯罪出发，对网络犯罪的停止形态与共同犯罪问题简要分析。

一、网络犯罪的停止形态问题

所谓故意犯罪的停止形态，是指故意犯罪在其发生，发展和完成的过程及阶段中，因主客观原因停止下来的各种犯罪状态，包括犯罪预备、犯罪未遂、犯罪中止和犯罪既遂四种形态。它们是故意犯罪已经停止下来的各种不同的结局和形态，属于相对静止的范畴。[1](p288)本文将讨论网络犯罪的预备、中止和未遂问题。

（一）网络犯罪中的犯罪预备问题

所谓预备犯是指已经实施犯罪预备行为，但由于行为人意志以外的原因，未能着手实行犯罪的犯罪形态。[2](p416)传统犯罪中预备犯的问题已早有相关论述，此非本文研究的重点。对于新刑法第285条和第286条规的新型犯罪，则颇有研究商榷的地方。

以刑法第285条规定的非法侵入特定计算机信息系统罪为例，有学者认为本罪是行为犯，只要查证行为人有侵入特定计算机信息系统的事实即构成犯罪既遂。[3]还有学者认为：本罪是行为犯，并且认为本罪的犯罪形态只有犯罪预备、犯罪中止和犯罪既遂三种状态，而没有犯罪未遂，判断犯罪预备与犯罪既遂界限的标准应当是行为人的侵入行为是否突破或绕过系统的安全机制。[4]

本文认为，不论是刑法立法还是刑事司法，针对网络犯罪必须充分考虑网络的特殊性质，而不能以传统的眼光与思路来分析处理此类新型犯罪。在网络环境中各种各样攻击行为很常见，都可能对网络造成一定的影响。如对此类行为规定为预备犯则将极大地扩张刑法对网络生活的干预度，而且即使规定了此类犯罪的预备犯，其预备行为也是难以准确认定与处理的，打击准备工具与制造条件的行为几乎等同于封杀网络生活本身。由于网络空间的庞大与广阔，对于预备入侵特定计算机信息系统的行为通常很难发觉，因此这些将给司法实践带来很大的困扰和不确定性，况且这些行为距离具体犯罪是较远的，也未造成直接威胁或较大损害。如果说有威胁的话，网络上的威胁可谓无一日不在。因此对于此罪不宜划分预备犯，否则打击面过于宽泛且实践中无法操作。同样，这些网络犯罪的特殊性在破坏计算机信息系统、数据与程序罪与施放破坏性计算机程序罪中也是存在的，因此，也不宜划分预备犯。从刑法自身的角度而言，在现代法治社会，谦抑性是其应有的价值意蕴。[5](p76)刑法调整的范围和方法都应有一定的限度，不应过多的干预社会生活，当不是必须用刑法来调整的情况下，就不应考虑使用刑法，而应优先的考虑其他法律方法。因

为刑法虽然是国家拥有的强有力的保障手段，但并不是唯一的手段，而且尽管刑法的打击严厉，但发动起来却需要耗费大量的国家司法资源。在网络日渐普及的今天，对于天文数字般的网络行为，动辄采用刑罚手段去处理，就显得既不经济也不可行，且有严刑峻法之嫌，也有违现代法治精神。

（二）网络犯罪中的犯罪未遂问题

刑法第23条第1款规定：已经着手实行犯罪，由于犯罪分子意志以外的原因而来得逞的，是犯罪未遂。在此须对‘犯罪着手’的概念进行一下明确。刑法学界基本认为，应当以行为人的行为是否与具体犯罪的实行行为紧密相接为标准判断是否着手。对犯罪实行行为着手的认定应当把握：第一以法律规定的具体犯罪的罪状为依据，第二以实行行为的形式和内容为基础。[7](p300)

网络犯罪的具有虚拟性，时空跨越的特点，犯罪行为人与犯罪对象之间并不直接接触，而且通过网络连接的虚拟方式进行信息接触，这种接触存在着多种复杂的可能性，因此对犯罪着手的认定，不能以在网络中存在电子信息交换接触就简单地认定为犯罪着手。因为我们知道根据刑法第285条所保护的三大类特定计算机信息系统的特点，均拥有严密的防护措施，网络防火墙 的性能是很优越的，并且均设置多重安全保护措施，一般要实破多重口令密码才能进入，这中间需要多次或者连续攻击才能达到实破入侵的目的。因此简单的初步的信息接触不应认定为犯罪，因为其尚不足以对该类计算机信息系统造成直接的现实的危胁，只有当行为人采用连续攻击或者多次渗透的方法确实已对系统造成实际威胁时，才应认定为犯罪着手。

同样在破坏计算机信息系统、数据、程序罪中也存在此类情形。但本罪与侵入特定计算机信息系统罪的不同之处在于本罪犯罪对象更为广泛，不仅包括上述三类特定计算机系统，还包括其他非特定系统。

行为人在网络上实施破坏行为，通常首先要侵入对方的计算机信息系统，如果仅侵入尚未来得及破坏即被发觉的，则应区分两种情况：如果其侵入的是特定三大类计算机信息系统则构成侵入特定计算机信息系统罪；如是侵入的是其他计算机信息系统，则应认为是属于情节显著轻微，危害不大的行为，不构成犯罪。

如果侵入后开始实行了删除、更改、增加等犯罪行为，发出犯罪信息指令，而由于犯罪对象计算机信息系统的数据锁定、数据备份或者被及时发现中断连接等致使未能对计算机信息系统的功能、数据和程序造成损坏的，则同样应区分来看：对于非特定计算机信息系统而言，由于其自身的重要性和受刑法保护的程度远低于特定计算机信息系统，则在破坏性行为没有造成损害的情况下，应认为危害不大，不认定是犯罪；对于特定计算机信息系统来讲，因其重要性之所在，应该说此种行为的社会危害性是较大的，应当认定为犯罪未遂，因其入侵行为在先，应按照牵连犯处理原则，实行行为吸收未遂行为，定为侵入特定计算机信息系统罪。

施放破坏性计算机程序罪则有其特殊性。其犯罪行为表现为制作与传播两个方面。对于网络犯罪来说，主要表现为传播破坏性计算机程序。应该说明的是，在网络时代，破坏性程序的影响必须要通过传播才能实现。因为破坏性程序的制作往往是在单个计算机或局部网络中进行的，如不加以传播其真正破坏力是无从体现的，因此制作后最终只有通过传播才能造成严重后果。没有了网络传播途径，再多的破坏性程序也不会对其他的计算机信息系统造成危害，因此在本罪的行为中传播才是关键。本文认为对于破坏性计算机程序的制作者，其如果是出于过失，当然不构成犯罪，如果是出于故意但并没有加以传播，也不宜以犯罪论处，但如将该破坏性程序提供给他人传播，则可认定为共同犯罪的帮助犯。

在网络中传播破坏性计算机程序的行为，由于网络的联结性，其危害的对象是极其广泛的，既包括特定三类计算机信息系统也包括其他计算机信息系统。事实上，网络犯罪中传播破坏性计算机程序罪是危害结果最为严重的一种，因此对其采用严格的刑法规制是必须的。正如同刑法中的危害公共安全罪一样，本罪危害的也是不特定多数计算机信息系统安全，该罪既是行为犯又是危险犯，只要行为人实施了传播破坏性程序的行为，就构成本罪犯罪既遂，因此本罪中不存在犯罪未遂与中止形态，也不应以严重后果为要件，如果造成严重后果则应加重处罚。如此既是对犯罪分子的一种震慑，防止这类具有极大危险的犯罪行为发生，同时也充分体现出刑法打击此类犯罪的态度和对公共利益的保护。当然在司法中对于破坏性程序要做出严格的限制和界定，应由计算机专家对破坏性程序做出准确评估鉴定，对于破坏性较小危害不大的，可不按犯罪处理，对于传播破坏性较大的程序应按破坏性质和程度分别量刑。

（三）网络犯罪中的犯罪中止问题

所谓中止犯是指在直接故意犯罪过程中，行为人自动放弃其犯罪行为或者自动有效地防止危害结果发生的一种犯罪形态。[9](p465)根据刑法规定可知：中止犯的构成必须具有时间性条件，自动性条件，有

效性条件。根据故意犯罪的过程划分中止犯又可分为犯罪预备阶段的中止，犯罪实行阶段的中止和实行终止的中止三种不同类型。

对于网络犯罪而言，主要存在的是实行阶段的中止和实行终了的中止。

关于侵入特定计算机信息系统罪，有学者认为：本罪不存在中止犯，只有未遂犯与既遂犯。[10](p210)也有学者认为在首次或前几次因意志外原因未能达到网络犯罪意图，在本来可以继续加以侵犯条件下放弃继续实施侵害行为可能性，从而使犯罪结果没有发生，由于行为人放弃行为出于本意，又仍在犯罪实行阶段，所以可以成立犯罪实行阶段的中止犯。[11](p44)应该肯定上述观点均有一定道理，但却失之全面。本文认为该罪中的犯罪中止是存在的，但要具体情况具体分析。在各种侵入行为当中，由于侵入者技术水平和设备的差异，有些侵入行为事实上是无法实现侵入的，并且行为人本身并未受到强制，仍存在继续发动攻击的可能，但其自动放弃的，其行为尚未对该罪所保护的法益造成直接现实的威胁，应当属于情节显著轻微，危害不大的行为，不应按犯罪处理。有些行为的物质技术手段足以侵入特定计算机信息系统，并且也实施了侵入行为，而最终行为人未能完成侵入行为是出于行为人的自动放弃，这种行为就对特定法益构成了直接现实的威胁，此情形作为中止犯处理就是合适的。由于侵入特定计算机信息系统罪的特点，只要非法侵入了特定的计算机信息系统，即已经构成犯罪既遂，故本罪不存在实行终了的中止。

对于刑法第286条规定的破坏计算机信息系统、数据、程序罪，有学者认为：行为人虽然实施了破坏计算机信息系统、数据、程序的行为，但没发生严重后果，就不能认为是犯罪[12](p612)，也有学者认为：行为人破坏非重要计算机信息系统功能，没引起严重后果的，不认为是犯罪；如行为人破坏三类特定计算机信息系统功能，在严重危害结果发生前自动放弃犯罪或者自动有效制止严重危害结果发生，应按中止犯处理。本文基本同意第二种观点，但又有不同之处。对于在网络环境下实施本罪，通常要先侵入计算机系统才能实施破坏行为，因此侵入是其先决条件。考虑到本罪犯罪对象范围比侵入特定计算机信息系统罪更为广泛，对此加以区分是正确的。对于普通的计算机信息系统而言，其系统的重要性和受刑法保护的程度与特定三类计算机信息系统是存在明显差别的。对于普通计算机系统，行为人虽实施了破坏行为，但并未发生严重后果，不论是行为人意志外原因还是自动放弃犯罪或自动有效防止犯罪结果的发生都可认为是情节显著轻微，危害不大的行为，不认为是犯罪。而对于三大类特定计算机信息系统则不同，由于受保护的是国家最重要的信息资源，保护的标准当然要远高于普通系统，并且行为人的主观恶性和危害程度也高于对于普通系统的犯罪。当行为人自动放弃犯罪或自动有效地防止严重危害结果发生的，按中止犯处理是恰当的，但由于侵入行为在先，在处理上按照牵连犯处理原则，完成行为吸收未完成行为，应以侵入特定计算机信息系统罪处理。

对于施放破环性计算机程序罪，如前所述，本文认为不存在中止犯。

二、网络犯罪的共同犯罪问题

我国刑法第25条第1款规定：共同犯罪是指二人以上共同故意犯罪。从刑法的这一原则性定义分析可知，共同犯罪必须具备以下三个要件：必须是二人以上；必须具有共同的犯罪行为；必须具有共同的犯罪故意。现在的网络犯罪已呈现出由单一犯罪向共同犯罪发展的态势，因此刑法规定与共同犯罪的理论也需要与网络环境的特点相结合才能准确把握。下面仍以我国新刑法规定的三类计算机犯罪为模板进行分析：

（一）侵入特定计算机信息系统罪

本罪的问题在于如何确立主、从犯问题上，司法实践中较难把握。由于计算机网络用户登记的可匿名性，对于多数攻击者的身份是难以确定的，并且在网络环境下对系统的攻击往往经由计算机指令的形式来表现，如果多人对计算机网络信息系统同时侵入，则一方面其入侵指令的来源难以确定，另一方面各种指令的攻击力强度也很难判断，即很难准确判定哪条指令在入侵行为起主要作用，哪条只是起了帮助次要作用。在入侵犯罪行为中起的作用是通过各自的攻击指令实现的，而这些指令却具有隐蔽性和时效性，在攻击行为结束后很难追查。如果单凭行为人的技术水平即确定其在共同犯罪中的地位，一则技术水平的衡量确定是否准确，二则是有主观归罪的嫌疑。如果将其全部认定为主犯，则又有违客观公正的原则，会造成事实上的不公平。因此这是网络环境对刑法理论的新挑战。

（二）破坏计算机信息系统、数据、程序罪

同侵入特定计算机信息系统罪一样，本罪也存在主从犯确定的问题，但较之前罪又有所不同。因为侵入特定计算机信息系统罪的犯罪方法多表现为对系统防火墙等防护装置的连续攻击，其频繁度、时效性很强，而对于攻击指令的记录往往因防火墙损坏而丢失或被攻击者删除，因此其攻击作用的强弱较难认定。对于本罪而言，其主要表现为删除、更改、增减计算机系统功能、数据等犯罪方式，这些犯罪行为并不需

要多次重复，通常一次指令即可完成。因此对于其破坏性的大小较易分辨，相比较前罪来讲，本罪的主从犯是较易确定的。司法实践中本罪的难点也在于对破坏行为来源的确定上，即破坏性指令是哪个犯罪行为人发出的不易确定，但是随着技术的进步，网络功能的增强，对于犯罪人IP地址及其指令的记录技术已经开始有所突破，为此类犯罪的定罪量刑提供了较大帮助。

（三）施放破坏性程序罪

一般来说，本罪的实行犯多表现为在网络上不同地址各自施放破坏性计算机程序，因此实行犯均应按主犯处理。但随着技术的进步，出现了软件分解组合技术：即行为人为防止其施放的破坏性程序被发觉，事先将该程序分解成若干独立段落进行伪装，然后由不同地址加以施放在网络上进行链接重组，这样在实行犯中就有了分工合作问题。虽然如此，但总的来说仍可按其在共同犯罪中的地位作用做出区分，对于以传播程序为主的行为可按主犯认定，对于提供链接空间等技术帮助的可按从犯处理。

本罪按照共同犯罪分工划分与前两罪并无二致，但对于刑法第286条规定的制作破坏性程序行为也构成本罪的正犯，本文则有不同意见。随着网络时代的到来，计算机的单机时代已经成为历史，与计算机网络相比，单台计算机的信息量几乎是微不足道的。破坏性程序的破坏作用也正是随着网络的发展才逐渐引起了人们的重视。在今天的网络环境下，可以说破坏性程序的破坏力必须要通过网络传播才能充分发挥。准确地讲，本罪是现在的网络犯罪中后果最为严重的犯罪，这也是刑法之所以设立本罪的原因。而对于制作破坏性计算机程序的行为，如不加以传播其危害性是极为有限的，是无法造成严重后果的，其必须与传播行为相结合才能发挥作用。与传播行为相比，制作破坏性程序的行为仅仅是在客观上为传播行为提供了工具或技术上的支持，属于传播行为的帮助行为。因此在本罪中传播是主，制作是从，是帮助犯。如果制作行为主观是出于过失或者虽是有意制作但没有传播的故意，也并未主动提供给他人传播，那么就不应以犯罪论处，不能构成犯罪，而只是违反国家有关行政法规的违法行为，应依法进行行政处罚，其造成损失可通过民事诉讼解决。

Copyright @ 2003 All rights reserved 中国社会科学院法学研究所版权所有 请勿侵权
地址:北京市东城区沙滩北街15号 邮编:100720
RSS