



工具型网络犯罪的类别与司法适用

童德华 齐文远

网络犯罪一般包括：以网络为对象的犯罪和以网络为工具的犯罪。以网络为工具的犯罪，在犯罪类型上比较传统，但是在方式方法上，则与传统方法迥异，所以，在司法适用中，有一些基本问题需要解决。本文从工具型网络犯罪的分类出发，谈谈司法适用中关于网络犯罪常见问题的处理看法。

一、工具型网络犯罪的具体类别

在对工具型网络犯罪分类时，行为方法固有的特点是基本的前提，毕竟“利用或者针对电信实施的不同种类的犯罪，可以说是千奇百怪的，其中有些在本质上并不新鲜，新鲜的是手段。”PN Grabosk and R·G·Smith, *Crime in the Digital Age*, Transaction Publishers, 1998, p14~17。但工具型网络犯罪在方法上的特点，通常由行为对象的特性所决定的，所以，以工具型网络犯罪所侵犯或者可能侵犯的对象的特征为主要标准，适当兼顾手段特征进行分类，应该是比较合理、比较实用的。基于此，结合我国刑法之规定，笔者主张将工具型网络犯罪先从纵向上分为两个层次。

第一层次是基于虚拟空间和现实空间的界限，以构成犯罪的行为或结果发生的空间为标准，将工具型网络犯罪分为“预备性”工具型网络犯罪和“实行性”工具型网络犯罪。所谓“预备性”工具型网络犯罪，是指在虚拟空间实施一定的行为，必须在现实空间借助其他媒介得以延续，才会造成严重的危害结果或严重危险状态，并构成犯罪的行为。所谓“实行性”工具型网络犯罪，是指在虚拟空间实施的一定行为，依照刑法的规定，即可构成犯罪；或者在虚拟空间实施一定的行为，无需借助其他媒介就能引起现实危害或危险，并构成犯罪的行为。

工具型网络犯罪，大意上有三个步骤：第一步是进入网络系统；第二步是对网络信息系统施加原因力，如破坏、涂改、增删、毁弃信息等；第三步是由于网络信息系统被影响，从而引起由其支持的设备设施的运作发生混乱、或者发出错误的指令，进而导致出现危害结果或严重危险状态。前两步行为发生在虚拟空间，而后一步发生于现实空间。即行为人在虚拟空间的行为影响(前两步行为)，对“实行性”工具型网络犯罪来说，是完整的实行行为；对“预备性”工具型网络犯罪，则只具有预备的性质。可见，“预备性”工具型网络犯罪是结果犯或危险犯，而“实行性”工具型网络犯罪不限于结果犯或危险犯，还可以是举动犯或行为犯。

第二层次是基于工具型网络犯罪的行为对象的特性，进行不同的分类。

关于“实行性”工具型网络犯罪，其类别和简要意思如下：

第一是经济类工具型网络犯罪。具体包括：(1)盗窃罪，即以非法占有为目的，通过网络秘密窃取他人以数字形式体现的财物、盗用他人的网络服务、网络设备、线路，数额较大或

多次实施盗窃的行为；(2)诈骗罪，即以非法占有为目的，通过网络信息系统虚构事实或者隐瞒真相，骗取公私财物(包括以数字形式体现的财物)，数额较大的行为；(3)贪污、职务侵占罪，即具有特定身份的人员，利用职务或者业务上的方便，通过网络侵吞、窃取、骗取或者以其他手段非法占有以数字形式体现的公共财物或单位财物；(4)敲诈勒索罪，即以非法占有为目的，通过网络发出威胁或者要挟的指令，强索公私财物(包括以数字形式体现的财物)，数额较大的行为；(5)洗钱罪，即明知是毒品犯罪、黑社会性质的组织犯罪、走私犯罪的违法所得及其产生的收益，而通过电子银行以及其他的电子资金划拨形式，在网络中掩饰、隐瞒其来源和性质的行为。

第二是传播有害信息类工具型网络犯罪。具体包括：(1)煽动分裂国家罪，即在网上传播煽动分裂国家、破坏国家统一的言论；(2)煽动颠覆国家政权罪，即在网上传播以造谣、诽谤或者其他方式煽动颠覆国家政权、推翻社会主义制度的言论；(3)侮辱罪，即在网上传播公开散布贬低他人人格，破坏他人名誉的言论，情节严重的行为；(4)诽谤罪，即故意捏造并在网上传播散布某种事实，损坏他人人格、破坏他人名誉，情节严重的行为；(5)煽动暴力抗拒法律实施罪，即通过网络发布煽动群众使用暴力抗拒国家法律、行政法规实施的言论；(6)传授犯罪方法罪，即通过网络向他人传授犯罪方法的行为；(7)制作、复制、出版、贩卖、传播淫秽物品牟利罪，即以牟利为目的，在网上制作、复制、出版、贩卖、传播淫秽物品的行为；(8)传播淫秽物品罪，即在网上传播淫秽书刊、影片、音像、图片或者其他淫秽物品，情节严重的行为；(9)战时造谣扰乱军心罪，指在战时，通过网络造谣惑众，扰乱军心的行为；(10)煽动军人逃离部队罪，指在网上散布唆使、鼓动现役军人逃离部队的言论，情节严重的行为；(11)战时造谣惑众罪，指军职人员在战时通过网络造谣惑众，动摇军心的行为；(12)编造并传播证券交易虚假信息罪，是指在网上传播编造并传播影响证券、期货交易的虚假信息，扰乱证券、期货交易市场，造成严重后果的行为；(13)诱骗投资者买卖证券、期货合约罪，是指证券交易所、期货交易所、证券公司、期货经纪公司的从业人员、证券业协会、期货业协会或者证券、期货管理监督部门的工作人员，故意在网上提供虚假信息或者伪造、变造、销毁交易记录，诱骗投资者买卖证券、期货合约，造成严重后果的行为；(14)损害商业信誉、商品信誉罪，是指违反反不正当竞争管理法规，在网上捏造并散布虚假事实，损害他人的商业信誉、商品信誉，给他人造成重大损失或者有其他严重情节的行为；(15)虚假广告罪，是指广告主、广告经营者、广告发布者违反规定，在网上对商品和服务做虚假广告宣传，情节严重的行为；(16)煽动民族仇恨、民族歧视罪，即在网上传播散布具有民族仇恨、民族歧视的言论，情节严重的行为。

第三是非法占有信息型工具型网络犯罪。具体包括：(1)为境外窃取、刺探、收买、提供国家秘密、情报罪。是指为境外的机构、组织、人员窃取、刺探、收买、提供网络中的国家秘密、情报的行为；(2)非法获取国家秘密罪，即通过网络，以窃取、刺探的方法，非法获取秘密的行为；(3)非法获取军事秘密罪，即通过网络，以窃取、刺探的方法，非法获取军事秘密的行为；(4)为境外窃取、刺探、收买、非法提供军事秘密罪，是指为境外的机构、组织、人员通过网络窃取、刺探、收买、非法提供军事秘密罪；(5)故意泄露军事秘密罪，即违反保守国家秘密法规，故意在网络中泄露国家军事秘密，情节严重的行为；(6)过失泄露军事秘密罪，即违反保守国家秘密法规，过失导致在网络中泄露国家军事秘密，情节严重的行为；(7)私自开拆、隐匿、毁弃邮件电报罪，是指邮政工作人员私自偷阅、隐匿或毁弃他人电子邮件的行为；(8)侵犯通信自由罪，是指非法打开他人电子信箱，偷阅、隐匿、毁弃他人电子邮件，情节严重的行为。

第四是知识产权型工具型网络犯罪。具体有：(1)侵犯著作权罪，是指以营利为目的，未经著作权人或与著作权有关的权益人的许可，在网上复制发行其作品，出版他人享有专有出版权的图书，未经录音录像制作者许可在网上复制发行其制作的音像制品，或者在网上制售假冒他人署名的美术作品，违法所得数额较大或有其他严重情节的行为；(2)销售侵权复制品罪。是指以营利为目的，在网上销售明知是侵犯他人著作权的复制品，违法所得数额较大的行为；(3)侵犯商业秘密罪。是指违反国家商业秘密保护法规，通过网络窃取他人商业秘密，或在网上传播、使用或者允许他人使用以非法手段获得的商业秘密，或者违反约定、违反保守商业秘密的协议，在网上披露、使用或者允许他人使用自己掌握的商业秘密，给商业秘密权利人造成重大损失的行为。

第五是更改信息型工具型网络犯罪。具体包括：(1) 伪造、变造金融票据罪，即制造假的电子金融票据、变动真的电子金融票据的行为；(2) 伪证证据类罪，即在诉讼中，有关人员毁灭、伪造与案件有关的电子数据证据，依法构成犯罪的行为。

至于“预备性”网络工具犯，只要是与网络有关系的其他犯罪，大体上可一并包含在内。如利用网络侵犯人身型的犯罪，就包括：(1) 故意杀人罪；(2) 过失致人死亡罪；(3) 故意伤害罪；(4) 过失致人重伤罪，等等。再如，利用网络从事破坏交通工具、交通设施，劫持航空器，破坏电力、广播电视、公用电信设备设施等危害公共安全的犯罪也可包括其中。所以前面有学者提出网络犯罪侵犯了我国刑法分则的十大客体，其见解的确能说明问题。当然，有些“实行性”的工具型网络犯罪也可以表现为“预备性”的工具型网络犯罪。如诈骗罪，既可以在网上完成，也可以利用网络的媒介功能，使受害人产生错觉，从而“主动地”交付财物。只是“实行性”工具型网络犯罪发生的场所比较独特，我们可以称之为“虚拟空间”，所以，其犯罪的手法、对象、停止形态都更是特殊，故此把它们归纳到“实行性”工具型网络犯罪中。

二、工具型网络犯罪的一般司法适用原则

(一) 对传统刑法理论的基本态度

工具型网络犯罪在许多方面具有与传统犯罪的不同之处，对此，能不能继续适用传统的刑法理论呢？笔者认为，不宜采取简单的态度取舍传统的理论。事实上，问题的最终解决必须依靠传统的理论，只是这些理论在网络犯罪领域必须得到发展，在某些方面应当修正。其理由如下：

首先，传统刑法理论，特别是居于通说地位的理论，都经过了长期论证，并不乏真知灼见。从外在特征上讲，它们对于解决刑事司法中的难题都具有一定的积极作用。就本质特征而言，它们是人类基于特定的政治、经济、社会文化背景，为预防和惩治犯罪而提出的。任何时代的犯罪，它都是行为人社会危害性和人身危险性的统一。我们可以认为，某种社会现象之所以被规定为犯罪，是因为它具有某种社会危害性，实施该行为的人具有一定的人身危险性。在刑事立法中，规定某种行为是犯罪的实行行为、某种行为是犯罪的预备行为、某种行为是这类性质的犯罪，某种行为是另外一种性质的犯罪，一方面，是为了保护社会免受犯罪之苦；另一方面，也是出于注意对于行为人区别对待、尽可能保持刑法的谦抑性原则和人道原则。这是刑事立法和刑事司法的共通之处，也是法治国对于犯罪所采取的基本立场。网络时代的犯罪也不例外。虽然它有这样或那样的独特方面，但是，行为人的行为都存在社会危害性，行为人具有不同程度的人身危险性。为了控制这种行为的潜在危险性，必须对它进行刑事规制；但假若规制过于严密，一则会发生侵犯公民权益的后果，一则可能导致阻碍网络发展的局面，反而违背规制的目的。所以，认识网络犯罪，特别是工具型网络犯罪，并不能脱离传统的刑法理论。

其次，传统的刑法理论在回应工具型网络犯罪时，的确面临着一些困境，出现了须待创新的要求。工具型网络犯罪对于传统刑法理论“引起”的问题，概括起来有：第一，“实行性”工具型网络犯罪的停止形态问题。例如，网上盗窃他人的电子货币行为，何时算着手，既遂与未遂区分的标准是什么？第二，网络中公然传播有害信息犯罪，通常所需要的“公然”应如何理解？第三，网络财产犯罪有无犯罪对象？如果有，是电子货币还是电子货币的载体呢？第四，侵犯知识产权犯罪的对象具体包括哪些？第五，特定犯罪性质的认定？如诈骗和盗窃犯罪如何区别？对于这些问题，简单地依赖传统刑法的理论，很难对刑事司法产生裨益。

再次，创新刑法理论是其自身的使命使然。刑法理论的使命在于为刑事立法和刑事司法提供具有建设性的积极意见，而不是对现行刑法法规进行消极的“抵制”或一味地“保守”，这就要求不能不作分析地认定刑法理论不能适用于某种行为或某种现象，也不能认为刑法理论历来如此，不可更改。那么，对于工具型网络犯罪，一方面，要承认它与一般犯罪的共性，承认传统理论适用的普遍性和根本性；另一方面，还要承认它的特性，承认对它认定时不可照搬照套传统理论，否则，就无法解决上述难题。

(二) 关于实行行为的着手

犯罪的着手，是区分犯罪预备和犯罪未遂的界限，它是指“犯罪人开始实施刑法分则条文所规定的具体犯罪的实行行为”。马克昌主编：《犯罪通论》，武汉大学出版社1999年第3版，第439页。那

么，在工具型网络犯罪领域，实行行为从何时或何环节开始呢？

我们认为，首先，应该将现实性环节行为排除在外。原因在于：第一，现实性环节行为不具有实行行为的特点。实行行为的着手，也就是开始实施刑法分则的具体构成要件的行为。判断它时，既要考虑法律规定的具体罪状，还要考虑实行行为的内容及其形式。马克昌主编：《犯罪通论》，武汉大学出版社1999年第3版，第443～444页。也就是说

，要将行为法律上的形式特征和实质特征统一考察。现实性环节行为，还不具备接近犯罪对象的条件，也就不可能对犯罪的客体产生危害，从而不具备实行行为的危害性；而且这个阶段的行为，通常是虚拟性环节的行为创造条件，更符合犯罪预备行为的特点。第二，将现实性环节行为作为实行行为有违立法精神。《刑法》第196条第3款规定：“盗窃信用卡并使用的，依照本法第二百六十四条的规定定罪处罚。”即按盗窃罪论处。有这个规定，我们可以推断，行为人仅仅只是盗窃了信用卡，并没有使用的，就不宜作为犯罪论处，至少不宜作为犯罪的完成形态论处。这时，权利人的财产权利并没有遭到实质性的损害，顶多受到了一定的威胁，该威胁转化为实害还须行为人进行虚拟环节的行为。所以刑法的规定是正确的。它可以作为处理相似情形的参照。基于同样的道理，盗窃或骗取其他人的电子签名、数字密码等行为，对此若以犯罪的实行行为对待，就与刑法规定的精神相违背。第三，将现实性环节行为作为实行行为，会造成司法适用的难堪。假如把现实性环节行为作为实行行为，无疑就会提前考虑犯罪的预备行为，从而将一些无关紧要的行为当做犯罪行为，如伪造智能卡，是一种预备行为，若将其作为实行行为，就会将此前的购买材料的行为当做犯罪预备行为，也可以追究其刑事责任。而这种行为的法律意义并不重大，将其作为犯罪处理就不太合适。另外，将实行行为提前加以考虑，那么虚拟阶段的行为属于实行行为吗？如果是，就出现了两种性质的实行行为，这自然会支解刑法理论，也不符合刑法规定；如果不是，则只能作为实行后的行为，就不会再发生消极性的犯罪中止，假如行为人根本就没有实施虚拟性环节的行为，也仍然要视为犯罪既遂，这显然于理不通。

其次，进入网络系统的初始行为也不是实行行为。尽管进入网络系统距离行为人完成网上犯罪的时间极短，有时只有几秒钟，但是正确认识这种行为的性质还是必要的。之所以说它不是实行行为，原因之一在于，该行为不具备实行行为的性质。为了完成网络中的特定犯罪，行为人一般要进入特定的信息系统。在此之前，他也许还需登录其他具有辅助功能的信息系统。如在BBS上泄露国家机密的，他首先要进入因特网或者局域网，然后进入某网站，打开主页，之后才可到BBS上实施实质性的犯罪行为。此前的行为是必需的环节，而非能直接侵犯客体的行为，所以不能认为是实行行为。原因之二在于，从刑事政策的角度，排除这些行为具有实行性质，有助于防范行为人进一步实施犯罪行为。如果这个阶段的行为只是预备性的，那么无疑给了行为人相当充足的时间中止犯罪，从主观上促使其犯罪意图表征不完全。反过来看，这也有助于司法机关充分认定行为人的主观心态，为惩治犯罪提供更可信的证据。

我们认为，只有进入特定的信息系统后实施的虚拟性环节的行为才是实行行为。原因在于：

- (1) 该行为具有侵犯犯罪客体的现实性，如果不受其他因素的影响，它就会实施完毕；
- (2) 该行为具有刑法中实行行为的特征，即引起构成要件结果的直接行为。

(三) 关于犯罪未遂

区分犯罪既遂与未遂的标准，在学界有许多观点，如“犯罪目的实现说”、“犯罪结果发生说”、“犯罪构成要件齐备说”等。目前虽然最后一种观点暂居主导地位，但其他不同观点依然存在。马克昌主编：《犯罪通论》，武汉大学出版社1999年第3版，第445页。“犯罪构成要件齐备说”能够更加准确地认定犯罪的完成形态，进一步区

分结果犯(包括危险犯)与行为犯(包括举动犯)两种情形。对于工具型网络犯罪的完成形态，首先也有必要区别结果犯和行为犯两种情形。

对于结果犯而言，发生法定的危害结果或出现了法定的危险状态，是犯罪既遂的标准。然而该结果是发生在虚拟空间的还是发生在现实空间的呢？如盗窃电子货币，究竟是出现了电子货币从一个账户上转到另外一个账户上这个结果，还是权利人现实的财产出现了减少这一结果？这个问题的意义是不言自明的。我们主张，应当以现实空间发生的结果作为犯罪既遂的标准。

理由是：

第一，这与现代刑法的精神实质是一致的。现代刑法立足于保护社会的机能，兼顾人权保障的机能，二者不可偏废。为了达到这一目的，在刑事立法时，没有采取一刀切的方法，而是区别不同的犯罪类型，在既遂的界限上，有的要求特定的危害结果，有的要求特定的危险状态，有的只需要实施了一定行为，有的甚至只要求作出某种举动。这是因为考虑各种社会关系体现的社会利益大小差异，如此才能均衡刑法的机能。工具型网络犯罪侵犯的客体并没有超越一般犯罪的范畴，所以，在对结果的把握上，它如果背离其他犯罪的要求，另外确定标准，就会破坏现行刑法的均衡点，势必与现代刑法的精神发生矛盾。

第二，虚拟空间的结果向现实转换在时空上还存在隔离。虚拟阶段的结果仅仅表现为权利记载上文字或信息数据的改动，它是否必然损害权利人的权益，还必须依赖于行为人进一步深化行为，致使权利人实实在在的财物、人身、名誉等被侵犯，从而出现实实在在的现实结果，而行为的深化方法可由行为人自己完成，也可由他人完成，也可由工具实现。只是在这个阶段，行为人也可以作出新的举动，如重新作出举动，将先前行为所造成的虚拟性结果取消，还原为原来状态。这样，权利人很难觉察权利受到过威胁，一定的法益秩序也并不出现混乱。从刑事政策上看，也有助于行为人中止犯罪。

第三，也是多数学者担心的，如果按上述方法处理网络犯罪，不惩治在网络系统中实施的违法行为，无异于鼓励行为人犯罪。笔者认为，这倒没有担心的必要。我们可以将该犯罪的预备形态与破坏计算机信息系统罪，依据牵连犯处理的原则加以处断。

对于行为犯而言，只要求行为人的实行行为具备刑法分则规定的条件，就构成犯罪的既遂，所以谈不上犯罪未遂。

三、工具型网络犯罪的若干司法适用问题

(一)网络中的诈骗罪

网络中的诈骗罪，是以非法占有为目的，通过网络信息系统虚构事实或者隐瞒真相，骗取公私财物(包括以数字形式体现的财物)，数额较大的行为。它是一类罪，包括普通诈骗罪、金融诈骗罪、合同诈骗罪等罪。

这类犯罪，得益于网络对于金融业的改造。网络技术的发展，对于人类社会的生活方式、工作方式产生了巨大改变。在金融领域，这种影响更为明显。在当今金融市场中，几秒钟之内，就可以完成数以亿计的资金转移，电子信息处理技术使资金转移的成本几乎降为零，交易者只需要在计算机键盘上轻轻敲几下，就可以实现资金的转移。而且，资金交换是即时的，一天24个小时不间断。在这种背景下，在网上出现了形形色色的经济诈骗犯罪，其中比例最大的就是诈骗。自然而然，对于这种犯罪的研究可谓是当务之急。然而，在此我们所研究的主要是“实行性”工具犯罪中的诈骗罪，即在虚拟空间就可以完成的诈骗罪，而这一点很大程度上是网络诈骗对象所决定的。

我国刑法学界关于犯罪对象目前存在争议，有“有体说”、“效用说”、“持有可能说”、“管理可能说”等观点。通说认为，“犯罪对象是指刑法分则条文规定的犯罪行为所作用的客观存在的具体人或者具体物。”高铭暄、马克昌主编：《刑法学》，北京大学出版社、高等教育出版社联合出版2000年

版，第61页。这就将体现一定财富的电子符号，如电子货币等排除

在犯罪对象之外。而财产性犯罪通常是有犯罪对象的。这就造成传统刑法理论和网络现实的矛盾，以至于有学者在研究利用计算机盗窃电子资金时，提出应将电子资金作为盗窃对象，其理由是：第一，盗窃犯罪对象的内容应随着社会的发展进步而不断扩展；第二，电子资金不同于一般的知识信息，要将他人账户上的资金通过计算机秘密划拨到自己的账户上来，被害人账户上的资金必须相应减少，否则计算机拒绝运行；第三，电子资金在性质上和有价值支付凭证、有价证券、有价票证相同，后者既然可被视为犯罪的对象，也就没有理由拒绝将前者也作为犯罪的对象；第四，刑法和司法解释已经把电力、煤气、天然气和电信服务规定为盗窃罪的对象，所以也应当将电子资金当做盗窃罪的对象；第五，把电子资金归入盗窃罪的犯罪对象，有利于保护金融财产。皮勇：《论金融领域计算机犯罪》，载《法学评论》2000年第2期，第123页。我们认为，论者的主张是正确的，它不仅适用于盗窃犯罪，而且适用于一切“实行性”工具型的网络经济犯罪。这样，经济型工具型网络犯罪的对象就

是电子货币，即“存在于电子资金过户系统中代表一定的资产所有关系的电子数据记录”。

皮勇：《论金融领域计算机犯罪》，载《法学评论》2000年第2期，第121页。

为了更好地认识犯罪的对象，我们还要将电子货币和电子货币支付手段区别开。网络中常见的、具有法律意义的电子货币支付手段主要有如下种类：

1. 电子票证。常见的电子票证包括：用户意见及产品需求调查表、产品购买者信息反馈以及维修或保障信息反馈表、产品(商品)报价申请表、报价单、定货单。需要注意的是，电子数据交换(EDI)在不断完善、不断发展，其宗旨是彻底实现票证传输的电子化，也被称为“无纸化贸易”。在现阶段，由于传统观念和技术限制，还只能是电子票证和纸张票证同时使用。但是，如果着眼于长远，我们绝对不能否定电子票证对于犯罪的意义。事实上，在许多国家和我国的一些经济比较发达的地方，纸张票证已经从先前的惟一或主要地位降为次要或辅助地位，这很能说明问题。
2. 电子钱夹。它是通过网络系统的认证中心发放的，其中包含经过认证的信用卡、身份证等。使用者使用电子钱夹，可以随时随地完成操作，有关个人的、信用卡的、密码的信息直接传送到银行进行支付结算。
3. 智能卡。它可以在网络中直接进行小额现金支付，并可以通过因特网从银行账号上下载现金，保证电子现金使用的便捷性。它也可以附加密码，从而保证使用安全。除此之外，它还有身份鉴别、发放政府福利等功能。如在学校使用智能卡，可以验证教师、学生的身份；还可以作为电子货币，用来支付用餐、复印、洗衣等费用，甚至可作为宿舍钥匙。在美国，估计有80%的金融交易是电子支付的。PN Grabosky and R·G·Smith, *Crime in the Digital Age*, Transaction Publishers, 1998, p150.

4. 电子票据。票据包括汇票、本票和支票。电子票据主要是电子支票。早在1995年，美国一些大银行和计算机公司联合进行技术开发并公开演示了使用互联网进行的电子支票交易系统，并且预言：“这个系统可能会引起银行交易发生革命”。新加坡也于近年开发了亚洲第一套电子支票系统。在我国，因为受到1996年实行的票据法的制约，所以电子票据尚属空白。但是，我们确信，随着中国金融认证中心的建立和数字签名在电子支付中法律地位的确立，加之网络技术的发展和现实需求的加强，电子票据一定会成为未来的一种重要支付手段。

5. 电子银行账户。电子银行为企业或个人提供信息查询、货币支付、储蓄业务、结算、在线投资、理财管理等业务。其中，个人、公司企业的储蓄、资金划拨等在线支付必须通过权利人在电子银行上的账户。我们不妨将电子银行账户看做实现电子货币转移的基础。这些支付手段，一般都是有形的，它们是电子货币得以移转的载体。换言之，没有这些载体，是无法实现电子货币移转的。进而可以说，行为人进行经济型的工具型网络犯罪，要依赖这些载体。但它们不是犯罪的对象。因为它们并不直接反映财产关系或经济秩序关系的犯罪客体所受到的侵犯。如行为人窃取他人智能卡到他取现或进行使用之间，有时间上的间隔，在此期间，原持卡人可以挂失从而避免财产受损；或者行为人并没有利用智能卡，权利人的财产就没有受到损失。所以，决定是否对行为人追究刑事责任不是看他是否取得了电子货币的载体，而是他取不取用电子货币的现实可能性，以及他对于电子货币所体现的财产权施加危害的大小。

另外，盗取或者骗取他人网络服务。网络服务要在网络中计费，最终涉及的依然是以数字符号表示的财产关系，所以其犯罪对象也不妨看做是电子货币。

(二) 诈骗和盗窃的界分

依照传统的刑法理论界分诈骗罪和盗窃罪，似乎问题不大；但是在对盗窃信用卡后使用，以及盗窃空白发票、支票以及其他空白有价凭证然后使用的行为的定性上，也曾经出现过不同看法。新刑法颁布后所作的一些规定以及有关司法解释澄清了其中的一些问题，对于盗窃与诈骗的区别规定得更为明确。如刑法第196条规定，盗窃信用卡并使用的，依照本法第264条的规定定罪处罚。只是随着科学技术的进步，原本简单的问题在网络金融领域变复杂了。

信用卡是最早的电子货币载体，今天，体现电子货币的载体还包括其他的电子钱夹、电子票据和智慧卡，所以，犯罪的手段更是复杂、多样。如在日本，到处都有全国联网、各银行联网的现金自动取款机(ATM)，ATM和信用卡的普及程度非常高，针对ATM卡的犯罪也相当猖獗

，从盗刷他人的ATM卡然后破译密码，接着提取现金，发展到伪造主ATM卡，再发展到通过网络联结到银行的计算机信息系统直接窃取账户资金的“线上犯罪”。白建军主编：《金融犯罪研究》，法律出版社2000年版，第402页。还有一种行为人经常

使擅的作案方式，即在某处24小时监视受害者，乘机窃取其账号和密码，然后在网上利用这些窃取的账号和密码将受害人的电子货币划拨到自己的账号上。

区分的难点在于虚拟性环节的欺诈性与现实性环节的盗窃性竞合的场合。虚拟性环节是在网络中发生的，而现实性环节是在现实社会中发生的。

为了预防网络犯罪，在虚拟环节一般设置了一整套安全技术。第一是密码机制。对信息加密是最常用的安全交易手段，可以防范信息在传输和储存中的非授权泄露、对抗截收、非法访问数据库窃取信息等威胁。第二是数字签名技术。它是一组密码，发送人在发送信息时，将这组密码发出，收件人受到信息后，通过双方约定的法则进行运算，从而确定发送人的身份。在本质上，它类似于在纸张上的签名，既可确认信息是签名者发出的，又可证明信息自签发后到接收时未做任何修改。第三是时间戳。文件签署的日期和签名一样重要。在电子交易中，数字时间戳能提供电子文件发表时间的安全保护。第四是认证机制。它用来确认交易对方身份的真伪。第五是防火墙。这是一个防守性的技术措施，它是不同的网络或网络安全域之间的惟一信息通道，担负着防止外部攻击的使命。然而，这些安全技术决非完美无缺，每项技术都有破绽，这就为网络诈骗提供了机会。例如，篡改他人电子票据的数字签名，或更改电子票据的文义内容，再到电子银行骗取电子现金。

行为人为了取得或盗用他人的电子货币，在虚拟空间可以采取的方式有两类：一是破坏信息系统的正常运行，借机达到目的；二是冒充其他的权利人，骗取“系统管理者”的信任，从而获得或使用其他权利人的电子货币。用第一种方式达到目的的可能性在网络领域几乎是零，所以第二种方式是常见的。如此一来，肯定要使用欺骗性手段。为了使欺骗更有成效，尽快得到权利人的密码、签名等真实信息，无疑是行为人所追求的。有些行为人采取技术方式，在网络中破译权利人密码，套取其相关信息；也有的采取传统意义的盗窃方法获得这些关键信息。后一种情形就发生了盗窃行为和诈骗行为竞合的现象。

对此，立足于我国刑法的规定，结合传统的刑法理论，并充分考虑电子货币的特点，区分某种行为是属于盗窃罪还是诈骗罪，必须考虑发生在现实性环节的行为性质。因为通过前面的分析，我们可以看出，在虚拟空间发生的行为绝大部分具有诈骗的性质，但是，如果将网络经济型犯罪一律以诈骗罪论处，显然与法律的规定不符；另外，从法理上讲，盗窃罪相对于诈骗罪，属于重罪，当出现两种罪竞合时，要作为牵连犯处理，应定为盗窃罪。进一步说，在现实性环节发生的行为如果是诈骗，继之所为的虚拟性环节的行为就构成诈骗罪；在现实性环节发生的行为是盗窃，继之而为的虚拟性环节的行为就构成了盗窃罪。

具体而言：(1)对于使用未设定密码的智能卡，或者多次使用限额设定密码的智能卡的行为，只要达到较大数额，就构成了盗窃罪；(2)对于一年之内连续三次使用智能卡，应当认为符合《刑法》第264条规定的“多次盗窃”，构成盗窃罪；(3)盗用他人公共信息网络上网账号、密码上网，造成他人电信资费损失数额较大的行为，构成盗窃罪；(4)对于使用盗窃的电子钱夹，如信用卡等的行为，构成盗窃罪；(5)以虚假、冒用的身份证件办理入网手续并使用移动电话，造成电信资费损失数额较大的行为，构成诈骗罪；(6)骗取他人的各种支付手段的账号、密码，然后利用这些账号密码在网络中套取电子货币的行为，构成诈骗罪；(7)在网上采取技术方式，破译权利人密码，套取其相关信息，继而套取电子货币的行为，构成诈骗罪；(8)骗取智能卡的密码，继而使用的行为构成诈骗罪；(9)盗窃智能卡的密码，从而使用的，构成诈骗罪。

(三)网上侵犯著作权罪的对象

网上侵犯著作权罪的对象，存在很多问题。第一个问题是难以鉴别创作作品的作者，恰如B1 akenev所言：“数字技术混淆了作者和使用者之间的界限，操作和网络的结合导致了这样一种情形：一项作品中包含着许多人的智慧，从而引发了谁有资格抱怨盗用该作品的问题。”

PN Grabosk and R·G·Smith, Crime in the Digital Age, Transaction Publishers

，1998, p90. 第二个问题是哪些网上作品受法律保护。受法律保护的传统意义的作品有文学、戏剧、音乐或其他艺术作品，如音乐磁带、电影、电视广播等，现在，这些东西都能转换为数字信号在网络中传播，在何种途径下他们才能受刑法保护呢？在此，仅就我国刑法实践中迫切需要解

决的问题谈谈看法。

1. 关于计算机软件

首先，我们要确认计算机软件能够成为犯罪的对象。理由在于：第一，计算机软件受到我国法律保护。目前，《计算机软件保护条例》是保护计算机软件的实体性规定，它是《著作权法》的一部分。可见，我国对于计算机软件的法律保护也是通过著作权保护来实现的。第二，不对计算机软件进行刑事保护于理难通。计算机软件在现代社会具有重要地位，也是一项重要商品。为了开发研制软件，开发商要花费大量人力、财力、物力，而对于软件的利用、下载却是极其简单的。所以在许多时候，软件大量被他人使用，开发商却未得到应有的回报，这是不合理的现象。第三，国外对于网络的刑法保护可资借鉴。如在澳大利亚，自最高法院关于Auto desk Inc v Dyason(1992年)以来，未经授权拷贝计算机软件的行为就可视为违法。在美国，涉及计算机软件侵权的刑事、民事诉讼很多，如1993年“花花公子”状告多家单位，法院以严格责任判决花花公子胜诉。see PN Grabosk and R·G·Smith, Crime in the Digital Age, Transaction Publishers, 1998, p98~99.

其次，不宜将一切盗用计算机软件的行为都视为犯罪。“盗用”主要是非法下载或拷贝。第一，根据《中华人民共和国计算机软件保护条例》的规定，版权意义上的计算机软件是指计算机程序及有关文档，计算机程序是指，为了得到某种结果而可以由计算机等具有信息处理能力的装置执行的代码化指令序列，或者可被自动转换成代码化指令序列的符号化指令序列或者符号化语句序列，它包括源程序和目标程序。文档是指，用自然语言或形象化语言所编写的文字资料和图表，用来描述程序的内容、组成、设计、功能规格、开发情况、测试结果及使用方法。这是被保护的计算机软件的总体范围。第二，软件作为犯罪的对象，还有细究的余地。软件可以分为公用软件、商业软件、共享软件和免费软件。公用软件的版权已经被放弃，允许被复制、修改、演绎，所以不可能成为犯罪的对象。商业软件，受到严格的著作权保护，可以成为犯罪的对象。共享软件是一种处于调试阶段、供用户选择的商业软件，所以也可以成为犯罪的对象。免费软件是不收取费用让公众使用的软件，所以不宜作为犯罪的对象。第三，盗用商业软件或共享软件的行为，也不宜都作为犯罪处理。由于软件通常价格昂贵，而且随着时间得到不断改进，新版本的应用程序、更高级更强大的游戏、操作系统不断地产生新功能，如果一个消费者随时更新软件，那么一年中他至少每周得更换软件。这对于用户来说是难以为继的，所以，盗用软件的行为也就比较猖獗。在现实生活中，难于估计有多少人在盗用软件。所以，只有那些非法下载、拷贝软件，向公众转售，并以此营利的行为，才能构成侵犯著作权罪。至于为自己使用而盗用软件的，基于公平使用原则，不宜作为犯罪处理。在这里需要补充的是，侵犯著作权犯罪以营利的目的作为要件，是否妥当，值得怀疑。但是，不顾及刑法的规定做扩大解释，认为未营利的行为也要作为犯罪处断，也是不对的。

2. 关于数据库

网络数据包括两种：(1)是由单独具有著作权的作品集合而成的数据库；(2)是由不具有的事实或信息资料集合而成的数据库。见孙铁成著：《计算机与法律》，法律出版社1998年版，第26页。对于前一种，目前都认同它可以成为犯罪的对象；至于后一种，由于对其版权，具体为著作权的性质存在分歧，所以，其可否成为刑法保护的對象还未得到一致意见。

一种意见认为，只要数据库的开发者在开发过程中付出了一定的时间、经费和劳动，该数据库就具有原创性。而在网络数据的建立过程中，人们不仅要对于数据进行机械的录入，而且还要进行大量的技术处理，从而使数据库的资料成为按创建者的意图建立的一系列具有有机联系的数据的集合，这自然需要花费人们大量的精力和代价，所以数据库具有原创性。见孙铁成著：《计算机与法律》，法律出版社1998年版，第26~27页。

进而言之，对于数据库的非授权利用可构成犯罪。

另一种意见认为，只有在信息的选择和安排上体现了一定的创造性的数据库才具有原创性，只有这样的数据库才能受到法律的保护。见孙铁成著：《计算机与法律》，法律出版社1998年版，第27页。换言之，非授权利用数据库的行为，只有部分可

构成犯罪。

我们认为，对于数据库进行区别保护的刑事政策是可取。原因在于：第一，数据库的特点决定了对其加以刑事保护的必要性。正如第一种意见所说，数据库的建立要花费大量的财力、人力。在建立过程中的编排、组织、处理并非单纯的体力，而是技术性极强的工作。具有这种特征的数据库，和原创性作品的性质没有多大差异。将其加以刑法保护符合维护著作权的要求。第二，有些数据库，其建立的初衷是方便使用者，就好比路线的指示牌，其中难以体现作为著作权所必需的原创性，对此加以保护的意義不大。如“现在在澳大利亚，对于计算机数据库，只有在创建中付出了相当程度的劳动和技术，其选择和整理的材料使它可被视为原创作品时，才被保护。版权法评议委员会最近提出，是否要修订澳大利亚立法，以明确保护计算机数据库，但是最后的决定反对修改法律，理由是，现有条文提供了充分的保护。”

PN Grabosk and R·G·Smith, *Crime in the Digital Age*, Transaction Publishers, 1998, p101. 第

三，由于对于网络的社会影响，还有许多未知的因素，如果贸然进行刑法保护，有时还会妨碍网络的技术进步，违背立法意图。所以，有限保护是必要的，但要立足于充分认识的基础上。

(四)关于电子签名

在网络中确定权利、义务的主要手段是电子签名。它有时是进入特定信息系统的钥匙，有时是利用网络信息系统的屏障，有时是从事网络活动的标记。电子签名是一组特殊排列的数字，电子签名技术的发展，对于刑法解释传统的伪造、变造内容以及金融诈骗犯罪将会产生更为深远的影响。

过去，刑法理论和司法实践中，将伪造解释为仿制，而变造是改变真实的外观或内容。这种解释在我国《票据法》颁布后，存在明显不足。当时在理论界认为，伪造票据是指行为人仿照真实的汇票、本票、支票的形式、图案、颜色、格式，通过印刷、复制、绘制等制作方法非法制造以上票据的行为。变造票据是指行为人在真实的汇票、本票、支票的基础上或者以真实票据为基础材料，通过剪接、挖补、覆盖、涂改等方法，对票据的主要内容非法加以改变的行为。见郎胜主编：《〈关于惩治破坏金融秩序犯罪的决定〉释义》，中国计划出版社1995年版，第74页。然而，伪造票据的应然之义是模仿他人的签名、伪刻他人的印章、盗用他人真正的印章；变造票据是指依法没有变更权限的人，在有效的票据上，变更除签章以外的其他记载事项，从而使票据上的权利义务内容发生变化的行为。刘颖、童德华：《票据伪造变造辨析》，载《华中师范大学学报·哲学社会科学版》1996年专辑，第26页。这可引申出伪造变造票据的行为只是一种典型的票据欺诈行为，而不是独立于票据欺诈之外的与伪造变造货币的类同行为。所以，我们认为刑法的规定不大妥当。但是认识网络的犯罪，即使依照后者的观点，也会出现难以回答的问题。

以往的票据认证主要用手写签名。签名的书写随意性很大，并且中文的方块字极易模仿。盖章也是一样，几乎没有一种公章不能被私刻。系统采用计算机自动识别签名和盖章印章，提高了工作的效率，但是只要票据真伪的凭证仍然是签名盖章，就必然有不法分子试图模仿签名和私刻印章，同样也还有不法分子试图改造和涂销票据。近年来，一些不法分子采用计算机扫描，计算机刻章技术，使得私刻印章实现了电子化和自动化，完全可以以假乱真。因此，印章自动识别系统与签名盖章系统一样，绝对不是票据认证系统今后发展的方向。所以，密码机制和电子签名在网络活动中的意义被赋予了新内容。如收票人事先根据票据号编制密码，通过安全的信道，传送给出票人。出票人每次签发一张票据，就根据票据号，粘贴上密码。收票人根据票据号和密码的对应关系来验证票据的真伪，以防止第三者伪造票据。在金融机构则可开发变码印鉴系统，又称为密码支付系统认证票据。它采用传统的单钥密码体制。出票人和收票人事先约定一个密钥，由他们各自保存。出票人每签发一张票据，他先把票据内容数字化，然后他再用保存的密钥、链路加密报文，得到一个鉴别码，把它作为票据真伪的凭证，同票据一起传送给收票人。收票人重复同样的计算过程，又得到一个鉴别码，只要两个鉴别码相同，就认为票据是真实的。由于鉴别码是密钥和报文的函数，因此，报文的任何变动都会改变鉴别码，而且不使用密钥是无法计算得到鉴别码的。如此一来，传统的解释几

本上没有应用的价值了。这时，伪造将很困难，或许就不可能，但是，变造和传统伪造的内容如何界分有会很困难。

（童德华系中南财经政法大学法学院副教授、法学博士；齐文远系中南财经政法大学法学院教授、法学博士、博士生导师，中国法学会刑法学研究会常务理事）

更新日期：2007-2-10

阅读次数：774

上篇文章：拐卖妇女、儿童罪既遂与未遂的认定问题

下篇文章：对完善我国缓刑考察制度的几点思考

 打印 |  关闭

 TOP

©2005 版权所有：北京师范大学刑事法律科学研究院 京ICP备05071879号