



最新法律文件解读丛书

# 刑事法律文件解读

## 【司法解释、司法解释性文件与解读】

解读《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》

履行法定职责 更加全面正确有效地实施好法律

——最高人民法院研究室负责人解读《人民法院加强法律实施工作的意见》

## 【地方司法业务文件与解读】

让虚假诉讼者付出沉重代价

——解读《关于预防和惩处虚假诉讼的暂行规定》

## 【最新立法司法动态与解读】

我国刑事诉讼制度的一次重大改革

——全国人大常委会法工委负责人谈《刑事诉讼法》修正案（草案）

## 【司法工作热点问题研究】

侵犯知识产权两个司法解释实施后争议及反思

——兼谈销售他人复制的盗版音像光盘如何定性

## 【新类型疑难案例选评】

靖江启航特种运输机械有限公司、钱卫建等逃税、挪用资金、隐匿会计凭证、会计账簿案

〔评析〕行政处罚、处理是逃税罪刑事追诉的前置程序

主编/张 军

2011年·第10辑

(总第76辑)

元 出版社

## 图书在版编目(CIP)数据

刑事法律文件解读. 总第76辑/张军主编. —北京: 人民法院出版社, 2011. 12

(最新法律文件解读丛书)

ISBN 978 - 7 - 5109 - 0354 - 0

I. ①刑… II. ①张… III. ①刑法 - 法律解释 - 中国  
②刑事诉讼法 - 法律解释 - 中国 IV. ①D924.05②D925.205

中国版本图书馆 CIP 数据核字(2011)第 257440 号

刑事法律文件解读. 总第76辑

主编 张 军

---

责任编辑 兰丽专

出版发行 人民法院出版社

地 址 北京市东城区东交民巷27号 邮编 100745

电 话 (010)67550626(责任编辑) 67550558(发行部查询)

65223677(读者服务部)

网 址 <http://www.courtbook.com.cn>

E - mail [courtpress@sohu.com](mailto:courtpress@sohu.com)

印 刷 北京人卫印刷厂

经 销 新华书店

开 本 787 × 1092 毫米 1/16

字 数 140 千字

印 张 8

版 次 2011 年 12 月第 1 版 2011 年 12 月第 1 次印刷

书 号 ISBN 978 - 7 - 5109 - 0354 - 0

定 价 16.00 元

## 卷首语

《最新法律文件解读》是一套以为最新法律规范提供同步“解读”为主的系列丛书,分为刑事、民事、商事、行政与执行4个分册,按月出版。

本丛书以“解读”为重点,突出全、专、新、快、准等特点,通过对最新出台的法律、法规、司法解释、部门规章以及重要地方性法规进行同步动态解读,弥补了法律、法规、司法解释汇编类出版物没有同步阐释、解读内容的不足,为广大读者学习理解最新法律规范,正确贯彻执行法律文件,及时解决实践中的新情况、新问题,提供一个全方位、多层面的法律信息平台。

为依法惩治危害计算机信息系统安全犯罪活动,维护正常的计算机网络运行秩序,2011年8月1日最高人民法院、最高人民检察院联合发布了《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》,刑事法律文件解读(2011年第10辑)专门约请了该司法解释的主要起草人就其制定背景、内容和起草中的主要考虑等问题进行了深入的解读,以便读者在司法实践中准确理解和适用。另外,本辑还重点收录了最高人民法院《关于人民法院加强法律实施工作的意见》及解读和江西省高级人民法院江西省人民检察院、江西省公安厅、江西省司法厅《关于预防和惩处虚假诉讼的暂行规定》及解读,以飨读者。

D924.05

2011/0

· 76

阅 覽

## 《最新法律文件解读》丛书 编 委 会

(按姓氏笔画为序)

孔祥俊	任卫华	孙际泉	刘贵祥
刘德权	杜万华	杨万明	杨亚平
张益民	宋晓明	罗东川	周 峰
郑学林	赵大光	胡云腾	俞灵雨
宫 鸣	姜明安	高贵君	高憬宏
裴显鼎	戴长林		



责任编辑 兰丽专

电 话 (010)67550626

邮 箱 lanlizhuan@sohu.com

# 目 录

## 【司法解释、司法解释性文件与解读】

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

(2011年8月1日) ..... 1

解读《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》 ..... 喻海松 5

最高人民法院 最高人民检察院 公安部

关于信用卡诈骗犯罪管辖有关问题的通知

(2011年8月8日) ..... 24

最高人民法院

印发《关于人民法院加强法律实施工作的意见》的通知

(2011年8月1日) ..... 25

履行法定职责 更加全面正确有效地实施好法律

——最高人民法院研究室负责人解读《人民法院加强法律

实施工作的意见》 ..... 31

## 【最高人民法院典型案例公布】

最高人民法院

公布九起反规避执行典型案例 ..... 35

## 【部门规章、部门规章性文件与解读】

公安机关强制隔离戒毒所管理办法

(2011年9月28日) ..... 43

## 【地方司法业务文件与解读】

- 江西省高级人民法院 江西省人民检察院  
江西省公安厅 江西省司法厅
- 关于印发《关于预防和惩处虚假诉讼的暂行规定》的通知  
(2011年8月30日) ..... 52
- 让虚假诉讼者付出沉重代价  
——解读《关于预防和惩处虚假诉讼的暂行规定》  
..... 廖志坚 欧阳军 57

## 【最新立法司法动态与解读】

- 我国刑事诉讼制度的一次重大改革  
——全国人大常委会法工委负责人谈《刑事诉讼法》  
修正案(草案) ..... 64
- 全国律协关于《中华人民共和国刑事诉讼法修正案(草案)》  
的修改意见 ..... 72

## 【量刑规范化典型案例评析】

- 姚尚旺故意伤害案 ..... 李 峰 陈 瑶 93
- [问题提示] 故意伤害案件的一般量刑方法是什么?  
在量刑中如何适用限制刑事责任能力情节?
- 顾金伟、张阳强奸案 ..... 章 波 周 军 98
- [问题提示] 合谋实施强奸犯罪案件的量刑起点与单人  
强奸犯罪有何区别? 导致犯罪未遂的原因对量刑调节  
有何影响? 强奸实行犯与非实行犯在量刑调节方面是  
否应有所差别? 同时具有严重暴力犯罪累犯与自愿认罪  
两种相向情节时如何调节量刑? 帮助他人强奸自己前  
女友在量刑调节时应如何考虑?

## 【司法工作热点问题研究】

侵犯知识产权两个司法解释实施后争议及反思

——兼谈销售他人复制的盗版音像光盘如何定性 …………… 张晓兰 104

## 【新类型疑难案例选评】

靖江启航特种运输机械有限公司、钱卫建等逃税、挪用资金、  
隐匿会计凭证、会计账簿案

[评析] 行政处罚、处理是逃税罪刑事追诉的前置程序

…………… 吴惠林 次仁昌布拉 109

被告人孙某某、颜某某、卢某某招摇撞骗罪案

[评析] 冒充纪委工作人员“反腐”骗财构成招摇撞骗罪

…………… 代贞奎 118

## 司法解释、司法解释性文件与解读

# 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

法释〔2011〕19号

（2011年6月20日最高人民法院审判委员会第1524次会议、  
2011年7月11日最高人民检察院第十一届检察委员会第63次  
会议通过 2011年8月1日最高人民法院、最高人民检察院  
公告公布 自2011年9月1日起施行）

为依法惩治危害计算机信息系统安全的犯罪活动，根据《中华人民共和国刑法》、《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》的规定，现就办理这类刑事案件应用法律的若干问题解释如下：

**第一条** 非法获取计算机信息系统数据或者非法控制计算机信息系统，具有下列情形之一的，应当认定为刑法第二百八十五条第二款规定的“情节严重”：

- （一）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；
- （二）获取第（一）项以外的身份认证信息五百组以上的；
- （三）非法控制计算机信息系统二十台以上的；
- （四）违法所得五千元以上或者造成经济损失一万元以上的；
- （五）其他情节严重的情形。



实施前款规定行为，具有下列情形之一的，应当认定为刑法第二百八十五条第二款规定的“情节特别严重”：

（一）数量或者数额达到前款第（一）项至第（四）项规定标准五倍以上的；

（二）其他情节特别严重的情形。

明知是他人非法控制的计算机信息系统，而对该计算机信息系统的控制权加以利用的，依照前两款的规定定罪处罚。

**第二条** 具有下列情形之一的程序、工具，应当认定为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”：

（一）具有避开或者突破计算机信息系统安全保护措施，未经授权或者超越授权获取计算机信息系统数据的功能的；

（二）具有避开或者突破计算机信息系统安全保护措施，未经授权或者超越授权对计算机信息系统实施控制的功能的；

（三）其他专门设计用于侵入、非法控制计算机信息系统、非法获取计算机信息系统数据的程序、工具。

**第三条** 提供侵入、非法控制计算机信息系统的程序、工具，具有下列情形之一的，应当认定为刑法第二百八十五条第三款规定的“情节严重”：

（一）提供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身份认证信息的专门性程序、工具五人次以上的；

（二）提供第（一）项以外的专门用于侵入、非法控制计算机信息系统的程序、工具二十人次以上的；

（三）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身份认证信息的违法犯罪行为而为其提供程序、工具五人次以上的；

（四）明知他人实施第（三）项以外的侵入、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、工具二十人次以上的；

（五）违法所得五千元以上或者造成经济损失一万元以上的；

（六）其他情节严重的情形。

实施前款规定行为，具有下列情形之一的，应当认定为提供侵入、非法控制计算机信息系统的程序、工具“情节特别严重”：

（一）数量或者数额达到前款第（一）项至第（五）项规定标准五倍以上的；

（二）其他情节特别严重的情形。

**第四条** 破坏计算机信息系统功能、数据或者应用程序，具有下列情形之一的，应当认定为刑法第二百八十六条第一款和第二款规定的“后果严重”：

(一) 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；

(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、增加操作的；

(三) 违法所得五千元以上或者造成经济损失一万元以上的；

(四) 造成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；

(五) 造成其他严重后果的。

实施前款规定行为，具有下列情形之一的，应当认定为破坏计算机信息系统“后果特别严重”：

(一) 数量或者数额达到前款第(一)项至第(三)项规定标准五倍以上的；

(二) 造成五百台以上计算机信息系统提供域名解析、身份认证、计费等服务或者为五万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；

(三) 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；

(四) 造成其他特别严重后果的。

**第五条** 具有下列情形之一的程序，应当认定为刑法第二百八十六条第三款规定的“计算机病毒等破坏性程序”：

(一) 能够通过网络、存储介质、文件等媒介，将自身的部分、全部或者变种进行复制、传播，并破坏计算机系统功能、数据或者应用程序的；

(二) 能够在预先设定条件下自动触发，并破坏计算机系统功能、数据或者应用程序的；

(三) 其他专门设计用于破坏计算机系统功能、数据或者应用程序的程序。

**第六条** 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，具有下列情形之一的，应当认定为刑法第二百八十六条第三款规定

的“后果严重”：

(一) 制作、提供、传输第五条第(一)项规定的程序，导致该程序通过网络、存储介质、文件等媒介传播的；

(二) 造成二十台以上计算机系统被植入第五条第(二)、(三)项规定的程序的；

(三) 提供计算机病毒等破坏性程序十人次以上的；

(四) 违法所得五千元以上或者造成经济损失一万元以上的；

(五) 造成其他严重后果的。

实施前款规定行为，具有下列情形之一的，应当认定为破坏计算机信息系统“后果特别严重”：

(一) 制作、提供、传输第五条第(一)项规定的程序，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；

(二) 数量或者数额达到前款第(二)项至第(四)项规定标准五倍以上的；

(三) 造成其他特别严重后果的。

**第七条** 明知是非法获取计算机信息系统数据犯罪所获取的数据、非法控制计算机信息系统犯罪所获取的计算机信息系统控制权，而予以转移、收购、代为销售或者以其他方法掩饰、隐瞒，违法所得五千元以上的，应当依照刑法第三百一十二条第一款的规定，以掩饰、隐瞒犯罪所得罪定罪处罚。

实施前款规定行为，违法所得五万元以上的，应当认定为刑法第三百一十二条第一款规定的“情节严重”。

单位实施第一款规定行为的，定罪量刑标准依照第一款、第二款的规定执行。

**第八条** 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。

**第九条** 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、通讯传输通

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”。

**第十条** 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。

**第十一条** 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。

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中操作权限的数据，包括账号、口令、密码、数字证书等。

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。

## 解读

# 《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》

喻海松\*

为依法惩治危害计算机信息系统安全犯罪活动，维护正常的计算机网络安全运行秩序，最高人民法院、最高人民检察院联合发布了《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》（法释〔2011〕19号，以下简称《解释》），自2011年9月1日起施行。

\* 最高人民法院研究室法官。

为便于司法实践中正确理解和适用，现就《解释》的制定背景及经过、起草中的主要考虑、主要内容、时间效力等问题介绍如下。

### 一、《解释》的制定背景及经过

随着计算机信息技术和互联网业的快速发展，计算机信息系统在现代社会中发挥着越来越重要的作用，大量的经济活动、社会交往和日常生活都依赖于计算机信息系统的正常运行。计算机信息系统的普及在极大地方便了人民群众的工作生活的同时，其自身的安全问题也日益突出。为保护计算机信息系统的安全，《刑法》对危害计算机信息系统安全的犯罪作了规定：第二百八十五条对非法侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的行为作了规定；第二百八十六条对破坏计算机信息系统功能，破坏计算机信息系统中的数据和应用程序，制作、传播计算机病毒等破坏性程序的行为作了规定。针对维护计算机信息系统安全方面出现的新情况，《刑法修正案（七）》对《刑法》关于危害计算机信息系统安全的犯罪作了补充：在《刑法》第二百八十五条增加第二款，对违反国家规定，侵入第一款规定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，或者对该计算机信息系统实施

非法控制的行为作了规定；在《刑法》第二百八十五条增加第三款，对提供专门用于侵入、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、工具的行为作了规定。这些规定对于保护计算机信息系统安全，打击计算机网络犯罪发挥了重要作用。

2010年6月，国务院新闻办公室发表了《中国互联网状况》白皮书，维护互联网安全是其中的重要内容。据《中国互联网状况》白皮书，近年来，网络犯罪呈上升趋势，我国面临黑客攻击、网络病毒等违法犯罪活动的严重威胁，是世界上黑客攻击的主要受害国之一。据不完全统计，2009年我国被境外控制的计算机IP地址达100多万个；被黑客篡改的网站达4.2万个；被“飞客”蠕虫网络病毒感染的计算机每月达1800万台，约占全球感染主机数量的30%。据公安部提供的情况，近五年来，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、非法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。

目前，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，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，其含义需作进一步明确。(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，司法实务部门反映突出。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，在中央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，于2009年下半年启动了《解释》的制定工作。

“两高”抽调专门力量，负责起草司法解释。在充分了解当前危害计算机信息系统安全犯罪活动情况、司法实践遇到的问题的基础上，有关部门多次研究论证，拟出了解释初稿。2010年3月~6月，“两高”研究室会同公安部网络安全保卫局，对解释初稿进行了多次研究、修改，并前往案件多发地区进行调研，听取当地法院、检察、公安系统同志的意见。2010年7月~8月，将解释稿送请“两高”相关部门征求意见，并征求了全国部分高级人民法院、省级人民检察院和公安厅（局）的意见。根据反馈意见，形成专家论证稿，听取了赵秉志、陈兴良、张明楷等法律专家和方滨兴、季昕华等技术专家的意见，之后将解释稿送请全国人大常委会法工委刑法室、工业和信息化部办公厅、国家安全部法制办、国家保密局政法司征求意见。几经综合研究，反复修改，形成了《解释》（送审稿），分别于2011年6月20日由最高人民法院审判委员会第1524次会议、2011年7月11日由最高人民检察院第11届检察委员会第63次会议通过，自2011年9月1日起施行。

二、《解释》起草中的主要考虑  
为确保《解释》的内容科学合

理，能够适应形势发展、满足司法实践需要，我们在起草过程中，着重注意把握了以下几点：

1. 科学合理确定危害计算机信息系统安全犯罪的定罪量刑标准。为给司法实务提供可操作的定罪量刑标准，《解释》的不少条款都涉及数量或者数额。基于严厉打击危害计算机信息系统安全犯罪的考虑，我们立足司法实践，切实贯彻宽严相济刑事政策，对数量数额标准作出了相应规定。在制定过程中，我们组织专门力量深入司法实践，了解具体案件，为确定行为的社会危害性程度提供了依据，并充分听取了各方意见，最终确定了定罪量刑的相关数量或者数额标准。例如，根据数据的重要性程度不同对非法获取计算机信息系统数据罪的入罪标准予以合理区分，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十组以上的构成犯罪，而非法获取其他身份认证信息 500 组以上的构成犯罪；根据司法实践的具体情况，并考虑有效惩治和震慑非法控制计算机信息系统犯罪的需要，将非法控制计算机信息系统罪的入罪标准规定为 20 台以上。

2. 注重斩断危害计算机信息系统安全犯罪的利益链条。近年来，危害计算机信息系统安全犯罪猖獗和泛滥的深层次原因，是形成了环

环相扣的利益链条。因此，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，这是制定《解释》所要解决的核心问题之一。《解释》的相关规定明确了制作黑客工具、销售黑客工具、非法获取计算机信息系统数据、非法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种行为的刑事责任，有利于从源头上切断利益链条，有效遏制危害计算机信息系统安全犯罪的蔓延和泛滥。

3. 有效解决打击危害计算机信息系统安全犯罪司法实践中反映突出的法律适用问题。多年来，司法机关在办理危害计算机信息系统安全犯罪案件的过程中遇到了困难。在《解释》起草过程中，我们为适应司法实践需要，明确了危害计算机信息系统安全犯罪的定罪量刑标准，并特别解决了掩饰、隐瞒计算机信息系统数据、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、危害计算机信息系统安全共同犯罪的处理原则等长期困扰司法实践的突出问题。

### 三、《解释》的主要内容

《解释》共 11 个条文，大体而言，可以划分为如下三大块内容：（1）明确危害计算机信息系统安全犯罪的定罪量刑标准，对《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”的具体情形作出规定；(2) 界定危害计算机信息系统安全犯罪中术语的范围，对“计算机信息系统”、“计算机系统”、“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”等术语的内涵外延予以明确；(3) 解决办理危害计算机信息系统安全犯罪中有关法律适用疑难问题，对掩饰、隐瞒计算机信息系统数据、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、危害计算机信息系统安全共同犯罪的处理原则等问题作出明确规定。

(一) 明确危害计算机信息系统安全犯罪的定罪量刑标准

1. 非法获取计算机信息系统数据、非法控制计算机信息系统行为的定罪量刑标准

《解释》第一条共分为三款，明确了《刑法》第二百八十五条第二款规定的非法获取计算机信息系统数据、非法控制计算机信息系统罪中“情节严重”、“情节特别严重”的具体情形。

第一款规定了“情节严重”的具体认定标准。主要包括下列情形：第(一)项以获取网络金融服务的身份认证信息的数量为标准。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，故应对身份认证信息予以重点保护。根据司法实践的情况，综合考虑行为的社会危害性，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10组以上即属“情节严重”。第(二)项以获取网络金融服务以外的身份认证信息的数量为标准。对于网络金融服务以外的其他网络服务，如网络即时通讯、网络邮箱等，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。获取其他网络服务的身份认证信息五百组以上的，应当认定为“情节严重”。需要注意的是，对于实践中发生的出于好奇、显示网络技术为目的而实施的打包盗窃论坛身份认证信息等行为，即使获取身份认证信息略微超过500组的，由于社会危害性也不大，也应当适用《刑法》第十三条但书的规定，不宜纳入刑事打击的范围。在司法实践中，要准确把握第(一)项和第(二)项规定的“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



计算机信息系统中操作权限的认证信息的一个组合，比如，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，则应认定为有效身份认证信息。第（三）项以非法控制计算机信息系统的数量为标准。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。为了解决上述问题，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20台以上的，应当认定为“情节严重”。第（四）项以违法所得或者经济损失的数额为标准。非法获取计算机信息系统数据、非法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，故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，即违法所得5000元以上或者造成经济损失1万元以上的，应当认定为“情节严重”。第（五）项是关于兜底条款的规定。此外，第二款根据计算机网络犯罪的性质和危害程度，并参照以往有关司法解释，以“情节严重”的五倍为标准，对“情节特别严重”作了规定。

明知是他人非法控制的计算机信息系统，而对该计算机信息系统的控制权加以利用，使得该计算机信息系统继续处于被控制状态，实际上是对该计算机信息系统实施控制，应当认定为非法控制计算机信息系统，故第三款明确规定对此种行为适用前两款关于非法控制计算机信息系统行为的定罪量刑标准。

2. 提供侵入、非法控制计算机信息系统程序、工具行为的定罪量刑标准

《解释》第三条共分为两款，明