社会科学研究中信息防护模式的探究

李福强

社科院 计算机网络中心

【摘要】随着网络和信息化的发展，人们对于网络和电子信息的依赖程度也越来越深。信息化技术改变了社科院科研人员的工作方式、提高了工作效率，与此同时也给研究工作带来了一系列新的问题。本文针对科研人员的在信息使用方面的主要工作特点，总结归纳了科研人员在使用计算机和电子信息过程时经常遇到的某些问题，并且针对这些问题介绍了我们所采取的解决方法，结合我院十年信息化建设的实际的工作情况，进而探究出一套适合社科院科研人员应用的信息防护模式。

【关键词】信息防护、网络基础建设、终端防护

计算机和网络，改变了人们的生活方式，它的影响正在一点点的加深，这使得绝大多数人已经无法摆脱计算机和网络。自 1998 年社科院的网络开通以来，计算机和网络开始在本院大范围的推广，随着发展和应用的深入，科研人员原有的工作方式和科研手段也在不断的改变。社科院网络中心作为全院唯一的一个网络和信息化专职单位，其主要工作职责是，制定社科院整体的信息化建设规划与开发、社科院的网络建设和管理、制定信息化应用和管理的相关标准与制度、组织业务培训等，最终实现支持科研、服务于全院科研人员的目的。

社科院，作为全国社会科学研究的最高学府，其工作重点就是对社会科学的研究。在科学研究过程中，主要工作流程就是信息的获取、使用和产生。而研究成果最终仍然是以信息的形式呈现出来。社科院以文科研究为主，和以理工类为

主的研究单位相比，社科院的科研人员在工作中对计算机和网络使用水平上相对来说要低一些，所以在使用计算机和电子信息过程中经常遇到这样或那样的问题。与信息相关的几个特点以及由于这些特点所带来的一些问题有：1、信息需求量大、范围广。因此社科院的学者在网上下载的信息量特别大，甚至下载一些视频信息，因此经常会引起网络堵塞；2、对外交流比较频繁。社科院的学者对外交流的主要方式是电子邮件，所以学者的电子信箱基本是公开的，获得这些信箱地址也很容易，因此社科院的电子信箱也就成为垃圾邮件的一个优先投送点；3、好奇心较重。特别是对于自己研究领域的信息好奇心就更重，网络上一旦出现自己感兴趣的相关信息就会去看，因此在浏览网页的同时也让很多的木马病毒乘机而入；4、外出调研多。多数学者在院内办公的时间较少，经常在院外办公，一些集中管理的软件在院外时就进入无安全控制的状态。因此经常出现在院外感染了病毒后，来到院里办公时就把病毒传给了院内的其它用户，甚至会导致全院网络瘫痪的问题；5、查杀病毒类工具软件使用水平不够。一些学者不会设置杀毒软件，甚至不知道杀毒软件需要更新病毒库和定期查杀病毒，一旦出现新的病毒时被感染的可能性很高，且一台计算机内还会出现多种病毒和上万个病毒感染文件；6、防护意识薄弱。比较突出的问题是，学者们在使用移动存储设备时，经常出现在别的计算机上使用后直接在自己的计算机上运行使用的现象，致使 U 盘病毒感染本机或传给其它用户，最终引起计算机系统出错、文件损坏或丢失。

以上列举的这几个主要问题，经常会给科研人员的工作带来不便、甚至是致命性的障碍。为了协助保障科研工作的顺利进行，社科院网络中心，在这十几年的工作过程中，针对科研人员的主要工作特点和遇到的问题，不断摸索创新，结合本院的实际情况，在信息防护方面采取了一系列行之有效的防护措施。主要包括网络的基础建设、终端防护控制、宣传教育、规章制度的完善。

一、 网络基础建设

网络基础建设是网络世界的基础，所有的应用及信息都是依附于这个基础而存在，网络基础没有建好必将给网络应用带来巨大的影响。网络中心从开始建网

就意识到了这点，在这十多年的发展过程中始终不断的加强网络基础建设。值得一提的是，结合社科院的实际情况，网络中心在基础建设这方面采取了一些大胆的创新举措。

在网络结构上，社科院采用了传统的内外网逻辑隔离的方式，但在 DMZ 区的建设上，建立了独立的 DMZ 区，即 DMZ 区与内外网分别设置在不同的防火墙上，并且设有单独的 IP 地址段。这样的设置可以有效的保护对外信息服务的正常运行，当内网出现问题时不会直接影响到对外的信息服务，特别是在网络拥堵时，不会因内网的防火墙的瘫痪而引起对外信息服务的停止。与之相反的，当对外服务受到攻击时，同样不会影响到内网的正常使用。

在网络设置上，社科院没有采用目前使用较多的自动地址分配的方式，而是采用了固定 IP 地址分配的方式。详细的讲，就是为全院五十多个单位分配了一个或多个地址段和 NAT 地址，每一段地址内都有各单位的唯一编号，甚至有的单位会在地址段内设有楼层编号。这种设置的目的主要是把各个单位区分开，在管理中可以很清晰的分辨出一个地址是属于哪个单位的，特别是在出现问题时可以很快的确定问题出在哪个单位，这能够很好的缩小查找的范围。同时这样的设置也可以保障其它单位网络的正常使用，特别是出现类似 ARP 病毒、共享传播类的病毒和内网对外发起攻击时，基本上受影响的只是一个单位，其它单位还可以正常工作，这在很大程度上缩小了影响范围。

垃圾邮件已经成为全球问题。为了更好的保障科研人员的对外交流，特别是通过电子邮件方式的交流，为了减少垃圾邮件对社科院科研人员在使用邮箱时的影响，社科院从 2005 年开始为社科院的邮件系统安装反垃圾邮件网关。考滤到社会科学研究的工作特点，由于社科院的研究范围很广，特别是对社会上一些敏感问题基本上都有所研究。那么，要达到防范垃圾邮件又要保证正常的科研交流的顺利进行的目的，在选择邮件网关时，我们放弃了当时应用广泛的关键词过滤的方式，而选择当时规模比较小的行为模式的过滤方式的邮件网关。目前社科院垃圾邮件过滤效果依然很明显，不仅过滤掉了大量的垃圾邮件，同时也过滤掉了病毒邮件，也减降低了通过邮件感染病毒的机率。

网络畅通是保障科研的基本条件，社科院作为一个研究机构，科研人员经常会在网上下载一些信息或观看一些视频，但大量信息的下载和在线视频应用占用了相当大的网络带宽，使得网络经常出现拥堵，至使工作中的一些正常应用无法使用。为了解决这个问题，我们在网络上架设了带宽管理系统，通过它可以有效的保证带宽的合理使用。这套系统主要目的就是在上班时间内限制一些不正当的应用，以保障上班时间正常应用不受下载和视频的影响，使得科研人员能够比较快捷的获得所需要的信息，而下班后这些限制会完全放开，对于大量的信息下载可以在下班之后进行。

二、 终端防护

社科院科研人员在工作中所使用的信息以及研究成果大部分是保存在个人计算机，所以终端防护是保护科研信息的主要手段。对于终端用户威胁最大的就是计算机病毒和木马，对于这个问题的最好最简单的解决办法就是，为终端计算机安装杀毒软件和操作系统补丁。为了加强终端的防护能力，2004 年社科院开始调研网络版杀毒软件，并通过将近一年的测试和试用，在年底时利用两套杀毒软件，建立了社科院杀毒软件统一管理系统。为了加强防护能力和科研人员的防护意识，社科院利用强制安装的方式向全院推广这两款杀毒软件，经过近两个月的安装过程，社科院杀毒软件安装率达到了 90%以上。通过这次的强制安装，不仅加强了防护能力，更重要的是加强了科研人员的防护意识，现在已不再要求强制安装统一购买的杀毒软件了，但科研人员在新购计算机或重新安装操作系统时都会自觉的安装杀毒，并且能够做到定期升级病毒库和查杀病毒。

为了能够很好的解决系统补丁更新的问题，网络中心也作了很多的调研。在当时，比较好的解决系统漏洞问题就是到微软网站上进行自动更新，但由于要下载的补丁较多，一是需要的时间比较长，二是占用网络资源较多，不太适合社科院的实际情况。另外的一种解决办法就是使用微软的 SUS 或 SMS 系统，但这两个都是基于微软件的域管理下的补丁升级系统，如果在社科院内应用，就要新建 50 多个域，而且要求使用者都加入域，这在当时是很难做到的。为了解决这一

问题，我们通过网络了解到了上海交通大学有自己的解决办法，于是我们与上海交大的老师进行了联系，说明了我们的需求，最后他们根据我们的需求专门为我们制作了系统补丁升级客户端，利有这个客户端社科院所有员工都可以通过内网进行补丁升级，大大加快了升级速度减少了因升级带来的网络资源的占用。随着新的技术的发展，我们已将原来的 SUS 升级到了 WSUS，但我们还一直沿用这个客户端，利用它为我院内部计算机的操作系统升级系统补丁，实现了补丁的自动分发。

三、 宣传教育

宣传教育的主要目的在于，提高科研人员在使用网络、信息和计算机时的使用水平，社科院的科研人员们把绝大部分时间和精力都花在了科学研究上，而网络和计算机只是科研辅助工具，科研人员没有过多的学习如何更好的使用、维护计算机，加之网络和计算机的高速发展，使得学者们对网络和计算机应用水平相对较低、防护意识不够强。

为了帮助科研人员自如的使用计算机及网络，遇到问题得以及时的解决，在社科院院内建立了网管员制度。全院每个单位至少有一名专职或兼职的网管员，网管员负责本单位的网络和计算机的基本维护。为了提高网络管理员的应用水平，网络中心每年都会组织网管员技术培训，当社科院引进新的应用系统和新的软件时，网络中心都会组织网管员进行使用培训，并且在每次的培训中都会介绍一些防范技术和防范手段。除了培训，网络中心还经常组织技术交流，让大家能够了解新的技术和新的理念，同时利用内部网络或邮件系统发部一些新的问题以及解决办法。网络中心做这些的目的就是在于提高网管员的应用水平及防护意识，当网管员的水平提高了才能更好的为科研人员服务，同时也可以在日常的工作中不断的去影响科研人员，使得科研人员的应用水平和防护意识有所提高。

四、 规章制度建设

俗话说「没有规矩，不成方圆」，规矩也就是规章制度，是我们应该共同遵守的，用来规范我们行为的规则、条文，它是我们正常工作的保证。网络中心针对不同的业务系统制定了不同的管理制度，如：网站管理制度、信息发布管理制度、机房管理制度等。同时也根据一些具体的应用制定了具体的管理制度，如：邮件帐号申请制度、上网认证帐号申请制度、杀毒软件管理制度等。建立这些制度目的就是要规范办事流程，这不仅是规范用户也规范了管理者，随着技术和应用不断的发展，网络中心也在不断的修改和完善这些制度，使之能够更加适合社科院的工作需要。与此同时，社科院的所有人员也逐渐的严格的履行各项规章制度，使得网络的使用越发顺畅。

社科院的研究范围使得科研人员必需面向全社会，科研人员所需要的信息也多是来自于社会，所以社科院的网络也要面向社会开放，可以说目前网络上的所有的应用都要对科研人员开放，一旦有所限制都有可能影响到科研人员的日常工作。但是这种全开放又会给网络的可靠性带来隐患，于是有效的防护措施必不可少。网络中心在这十多年的信息化建设的过程中不断成长，在实践中探索出了一套适合本院的信息防护模式。在这个防护模式中，我们主要的工作是防护而不是阻止。该模式不是一个单纯的管理模式，它是一个以技术为主管理为辅服务科研为目的的综合模式。该模式的主要结构是，以信息为中心，由网络基础建设、终端防护、宣传教育和规章制度组成的一个圆形防护圈。信息是这个防护模式的最终防护对像，是这个模式的核心。网络基础建设是这个模式的基础，其首要目的是确保网络及其相关应用的正常运行，其次是通过不断的对它进行完善以加强整体的防护能力，是针对信息获取和交流过程中的防护。终端防护是在网络之外的一层防护，它主要是在针对信息在使用和存储过程中主要的防护手段。宣传教育是对前两项防护的一个补充，通过提高科研人员的应用水平和防护意识，从侧面完善这一模式。规章制度是对整个模式保障，通过对它的不断完善，以确保各项措施的顺利执行，应技术无法实现防护目的时，它就是最好的解决办法，因此它是这个防护模式中不可缺少的一环。这个模式与其它相关模式最大的不同就是，加强了技术弱化了管理，这与最为普遍认同的「三分技术七分管理」正好相反，

因为网络中心是一个以服务为主的单位，我们对于科研是辅助服务而非管理。当然这个模式也不是一成不变的，这是目前较为适合社科院的一种模式，随着网络和信息化技术的不断发展，也会不断的完善。例如目前社科院还欠缺的一些系统，如：远程访问系统、应急响应系统、统一服务平台、信息集中存储、灾备等等，这些系统一旦通过论证及测试适合社科院，我想它们会逐步加入到这个模式当中去。可以想象，在不久的将来，这个信息防护模式会逐渐扩大，其防护能力也会进一步加强，更好的为科研工作服务。

【作者简介】

李福强　男

职　　称：社科院 计算机网络中心 助理工程师

研究领域：网络安全和信息防护

个人简介：2005 年 6 月毕业于长春工业大学（本科）

联络电话：86-010-85196463

联络信箱：lifq@cass.org.cn