虚拟社会管理面临的挑战与应对措施*

文/冯登国　苏璞睿
中国科学院软件研究所 北京 100190

【摘 要】虚拟社会已与现实社会紧密结合，虚拟社会的管理既是确保虚拟社会自身稳定、有序发展的基础，也是维护现实社会稳定和秩序的需要。虚拟社会的开放性、匿名性、高技术性等特点，给虚拟身份管理、网络犯罪治理、舆论引导与监管、网络空间安全等方面带来了诸多问题。针对这些问题，应从技术支撑平台、技术标准、法律法规等多方面采取措施，构建和完善虚拟社会管理体系，提高对虚拟社会的管理能力和水平。

【关键词】虚拟社会，社会管理，信息安全

DOI：10.3969/j.issn.1000-3045.2012.01.003


冯登国研究员

1 引言

近年来，互联网技术和应用发展突飞猛进，已经渗透到社会的各个层面，互联网自身也形成了一个庞大的虚拟社会。虚拟社会中的各种活动是现实社会的一种反映和延伸。虚拟社会活动主要基于互联网进行，由于具有开放性、匿名性及高技术性等特点，如何对虚拟社会进行有效管理是我们当前面临的新问题和新挑战。

* 收稿日期：2011年12月26日

虚拟社会的管理问题已经成为各国政府关注的焦点之一，美国、日本、韩国等国纷纷针对虚拟社会的安全、管理等问题出台了一系列的法律、法规，并积极推动相关技术研究和基础设施建设。2011年美国提出了“网络空间可信身份国家战略（National Strategy for Trusted Identities in Cyberspace (NSTIC)）”[1]，将虚拟社会的身份管理上升到国家战略高度。

近年来，随着我国互联网的发展，虚拟社会带来的一系列问题也引起了广泛关注，社会各界也在积极推动相关管理措施、法律法规和技术手段的出台和完善。但由于我国互联网发展迅速、规模庞大、问题复杂，现有的相关措施与现实需求仍有一定的差距，面临的挑战主要包括以下几个方面：

（1）虚拟身份管理问题。在互联网发展初期，互联网用户规模不大，主要用于简单

的信息共享，采取虚拟身份与真实身份分离的机制，较好地保证了互联网的开放性、匿名性等特点，在一定程度上促进了互联网的快速发展。但随着互联网的快速发展和虚拟社会的快速膨胀，现实社会中的人、事、物与虚拟社会的联系程度不断提升，加强虚拟身份的管理既是虚拟社会自身发展的需要，也是规范现实社会秩序与虚拟社会秩序的需要。但现有的虚拟身份管理体系已无法满足现实需要。首先，电子商务等应用使得现实社会的各类活动直接迁移至网络空间，这些应用需要有效的身份管理以实现虚拟身份与真实身份的可靠关联与验证；其次，网络空间中各类虚拟资产的价值与个人、机构的现实利益之间的关系越来越直接，加强虚拟身份管理，可更有效地保障虚拟社会中各用户的自身利益；最后，网络空间中各类矛盾也越来越突出，频繁出现一些用户过激行为对其他用户造成伤害的现象，加强虚拟身份的管理有利于利用法律法规对相关行为进行规范，更好地保证虚拟社会有序发展。虚拟身份管理已成为解决虚拟社会管理诸多问题的关键一环。

（2）网络犯罪治理问题。随着虚拟社会与现实社会联系程度的不断加深，赌博、诈骗等现实社会中的犯罪活动也在虚拟社会中不断出现，同时，虚拟社会作为新的社会形态，还出现了网络钓鱼、隐私窃取等新型犯罪形态。如今的网络犯罪活动已不仅仅为了炫耀技术，而是为了达到经济、政治、军事等特定的目的。近年来，网络犯罪频频发生并造成了巨大的经济损失。比如，2010年10月开始，阿里巴巴B2B平台发生系列跨国网络诈骗案，共涉及网络诈骗案281起，涉案金额达660余万美元。网络犯罪是高科技手段下的新型犯罪形式，由于网络的无边界性和匿名性特点，犯罪分子很容易实施跨地区乃至跨国的网络犯罪活动，并且网络犯罪过程具有很强的隐蔽性，加之电子证据的瞬时性，难以侦察和取证。这些特点使得网络犯罪成为当今世界各国普遍面临的重要问题之一。

（3）舆论引导与监管问题。我国的互联网规模正在快速膨胀，其舆论核心地位也在不断增强。据统计，2011年，我国互联网用户已突破5亿，其中微博/博客用户已达3亿，Youku等在线视频网站用户也超过3亿，互联网已成为最重要的舆论阵地之一[2]。互联网在信息发布的速度方面具有传统媒体不具有的快速优势，但由于虚拟社会行为仍缺乏有效的监管，个别人的不负责任行为可能给其他人、其他机构、甚至整个社会带来严重伤害。若是被一些别有用心的人或组织利用，则危害更为严重。近年来，虚拟社会中谣言四起、各类舆论事件不断，特别是微博、Facebook等社交网络的出现，大大加快了信息传播的速度，比如在近年来发生的“伦敦骚乱”、“占领华尔街”等事件中，网络新媒体均发挥了重要作用。虚拟社会的舆论引导与监管问题已成为确保虚拟社会稳定、有序、良性发展的关键问题之一，也是各国关注的焦点。

（4）网络空间安全保障问题。网络空间安全是虚拟社会有序发展的重要基础，但随着网络空间用户越来越庞大，网络应用越来越多，越来越复杂，网络空间的安全保障问题也越来越突出。虽然我国长期重视网络空间安全保障工作，但仍难满足互联网快速发展、技术不断更新的需要。近年来，各类软件漏洞频频出现，恶意代码、分布式拒绝服务攻击等恶性事件层出不穷，并且越来越多地呈现出大规模、协同化、高危害的特点。网络空间安全保障已成为确保虚拟社会稳定发展所要解决的重点和难点问题之一。

因此，本文将重点从虚拟社会的虚拟身份管理、网络犯罪治理、舆论引导与监督、网络空间安全保障体系建设等方面分析国内外的发展现状，并探讨分析我国虚拟社会管理面临的挑战及应对思路。

2 虚拟身份管理

美国、日本、韩国、欧盟等国和组织对虚拟身份管理问题都给予了广泛关注。美国等甚至将虚拟身份的管理提升至国家战略高度，2011年4月，

美国白宫正式公布了“网络空间可信身份国家战略(National Strategy for Trusted Identities in Cyberspace (NSTIC))”,指出可信身份是改善网络空间安全的基石,并进一步明确了行动路线图和各参与方的任务[1]。韩国政府从2002年起推动实施网络实名制,通过立法、监督、管理和教育等措施,对网络邮箱、网络论坛、博客乃至网络视频实行实名制管理。2007年7月起,《促进使用信息通信网络及信息保护关联法》规定韩国各主要网站在网民留言之前,必须对留言者的身份证号码等信息进行记录和验证。同时,为了保护留言者的隐私,韩国政府允许网民在通过身份认证后,用代码替代真实姓名留言。但在具体实施过程中,上述措施仍面临众多的问题和挑战。2011年7月,韩国最大的门户网站之一Nate和著名社交网站赛我网遭到黑客攻击,导致3 500万名用户的个人信息泄漏。韩国行政安全部于2011年8月11日介绍了其规划的“个人信息保护综合对策”,决定重新审定税收和金融机构在提供网络服务时需要验证个人身份信息的相关政策,个人或企业使用用户身份证信息需要事先获得政府批准;进一步完善搜集个人信息的相关制度,在技术层面采取有效措施应对黑客攻击等,以加强个人隐私保护。

长期以来,我国一直非常重视网络空间的虚拟身份管理问题,2004年,颁布了《电子签名法》,对数字身份的有效性、法律责任等方面从法律层面进行了明确描述。在2006年国办发布11号文《关于网络信任体系建设若干意见》等重要文件中,对我国网络空间信任体系进行了明确,并强调了其在网络空间建设过程中的重要性。近年来,我国在技术标准、管理规范、法律法规方面也在积极推动,2011年12月,北京市制定了《北京市微博客发展管理若干规定》,规定要求北京市行政区域内开展微博客服务的网站,任何组织或者个人注册微博客账号,制作、复制、发布、传播信息内容的,应当使用真实身份信息,不得以虚假、冒用的居民身份信息、企业注册信息、组织机构代码信息进行注册。这是我国在虚拟身份管理方面的一次重要尝试。

我国互联网发展迅速、规模庞大,问题复杂,目前的虚拟身份管理仍难以满足虚拟社会发展的需要。综合分析虚拟社会发展的需求和信息技术的发展趋势,应从以下几个方面加强虚拟身份管理工作:

(1)加强统一虚拟身份管理基础设施建设。用户的身份注册信息,尤其是真实身份认证信息的核实、保存和保护过程均需网络应用服务商自身实现。在当前大量网站的安全技术水平较为薄弱的情况下,由网站负责保存用户身份认证信息,一旦发生数据被盗的情况,容易造成大规模用户隐私泄露问题,如最近曝光的600万CSDN用户资料外泄事件,会对虚拟社会身份的安全性造成冲击。因此,建设统一的虚拟身份管理基础设施,便于集中管理身份认证信息,提高用户身份信息的安全性。

(2)加强虚拟身份管理法律法规、技术标准体系建设。法律法规和技术标准既是约束虚拟社会参与者行为的重要准则,也是指导虚拟社会如何实现安全、有序管理的重要基础。网络应用和安全问题层出不穷,带来的虚拟身份管理需求也千变万化。我国应在现有法律法规的基础上,进一步完善虚拟身份管理相关的法律法规和技术标准,以适应当前互联网应用的需求,包括虚拟身份与真实身份的关联问题、个人隐私保护问题、虚拟身份管理中各方的法律责任问题,等等。

(3)加强用户意识教育和相关应用的扶持。虚拟身份的管理涉及到虚拟社会的每

一个参与者，与现实社会类似，虚拟社会管理中各种规章制度、技术手段也需要用户的配合才能真正发挥作用。而一些服务提供商对虚拟身份管理也缺乏正确的认识，对一些管理措施存在一定的抵触心理，因此，加强网络用户的法律意识和安全观念，并为各种网络服务的使用者、提供者和监管者履行各自的职责提供相应的技术或管理手段支持，不仅能从源头上减少虚拟社会中的各种问题，也有利于各项虚拟社会身份管理措施有效发挥作用。

3 网络犯罪治理

现实社会中常见的犯罪问题在虚拟社会中都有所体现，比如色情、赌博、诈骗等等。虚拟社会中的各种犯罪活动涉及规模更庞大、涉及范围更广泛，例如，2010年江苏查获的一件网络赌博案件涉案金额就达36亿元，2011年公安部查处的某网络色情网站会员达千万人规模。我国的网络诈骗问题也很突出，例如，2011年11月国际反网络诈骗联盟推出的上半年网络反诈骗统计报告，专门指出我国的网络诈骗问题严重，网络诈骗数量较去年同期增长了44%[3]。虚拟社会中的问题也有一些特殊性，具有较强的技术性，具有更好的隐蔽性，涉及范围、规模更大，造成其破坏性更强，而现有的监管手段难于发挥作用。

为维护国家信息网络安全运行，世界多个国家根据自己特有的情况，各有侧重地采取了包括政策、法律、技术等在内的多种手段打击网络犯罪活动。2001年11月，欧洲理事会的26个欧盟成员国以及美国、加拿大、日本和南非30个国家的政府官员在布达佩斯共同签署了《网络犯罪公约(Convention on Cybercrime)》[4]。公约规定了电子证据调查制度等国家层面的措施，制定了打击网络犯罪的国际合作准则。这是全世界第一部针对网络犯罪行为所制订的国际公约，该公约的制订标志着网络犯罪定义在世界范围内得到承认和全世界联合打击网络犯罪的开始。2003年1月23日，欧盟在斯特拉斯堡通过了《网络犯罪公约补充协定：关于通过计算机系统实施的种族主义和排外性行为的犯罪化》[5]，对公约内容进行了补充和完善。

作为信息产业最发达的国家，美国已经建立了一整套针对网络犯罪的法律体系。从1986年的计算机诈骗及滥用法案(Computer Fraud & Abuse Act)、电子通信私有法案(Electronic Communications Private Act)以来，美国已确立了十几项有关网络安全的法律，其中最主要的是美国国会1988年开始实施的计算机安全法(Computer Security Act)。“9·11”事件后，作为加强安全防范的有效措施，美国参议院通过了爱国者法案(USA PATRIOT Act)，强化了政府对网络安全的监控和管制，为执法部门的调查认证，尤其是为互联网和电子邮件的调查取证扫清了法律障碍。此外，2002年10月美国国会还通过了反恐怖主义法案(Anti-Terrorism Act)，该法案将黑客攻击视为恐怖主义行为之一，并把打击网络恐怖主义列为其中的一项重要内容。

1994年以来，我国颁布了一系列与互联网管理相关的法律法规，以约束网络行为和打击网络犯罪，主要包括《中华人民共和国电子签名法》、《互联网信息服务管理办法》等。国务院新闻办公室2010年6月8日发布的《中国互联网状况》[6]白皮书提到：为有效打击网络违法犯罪活动，中国法律规定，对利用互联网和针对互联网的犯罪行为，依照《中华人民共和国刑法》的相关规定追究刑事责任；对不构成犯罪的，依照《中华人民共和国治安管理处罚法》、《计算机信息网络国际联网安全保护管理办法》等法律法规予以行政处罚；中国反对任何形式的网络黑客攻击行为。

如何有效地预防、打击和惩治网络犯罪是一项全球性课题，涉及法律、技术等多方面的内容。结合我国的实际情况，在网络犯罪治理方面需要开展如下几个方面的工作：

(1)提升网络犯罪检测和取证的技术能力。网络犯罪是利用信息技术实施的高科技新型犯罪形态，如何及时准确地检测网络犯罪活动，快速有

效地获取网络犯罪的证据，是打击网络犯罪分子、遏制网络犯罪行为的基础，只有管理者抢占了技术制高点，才可能有力震慑网络犯罪分子。因此，需要大力支持网络攻击检测、恶意代码分析、网络取证技术、数据来源追踪等技术手段的研究和相关工具的开发，支持具有自主知识产权的技术、工具、设备与系统的推广应用，有效提升网络犯罪的防范、侦察和取证能力。

（2）完善网络犯罪惩治法律法规体系。网络犯罪是现实社会犯罪活动的延伸，仅从技术层面难以防止网络犯罪的发生，还需要依靠法律法规，通过约束用户的网络行为预防网络犯罪，通过惩治网络犯罪分子打击网络犯罪。为此，需要制定完善的网络行为规范和网络犯罪惩治法律体系，通过规章制度约束网络用户的行为，明确界定违法的网络行为及其需要承担的法律责任，不仅可为有效打击网络犯罪提供法律依据，也可以为网络用户维护自身利益提供法律武器。

（3）加强打击网络犯罪的国际合作。网络犯罪具有跨地区、跨国界的特点，我国网民可能受到外国网络犯罪分子的侵害，外国网络犯罪分子也可能利用我国的网络设施开展犯罪活动。在打击传统的跨国犯罪活动中，有国际刑警组织等机构可以协调各国共同行动，而在虚拟的网络空间中，网络犯罪活动的这种跨国特性更突出、更显著，更需要国际间的协作和不同国家、国际组织的共同参与。

4 舆论引导与监管

近年来发展比较迅速的 Twitter、Facebook 等均属于社交网络，是一种新的媒体形式，由于其本身具有较高的用户聚集密度和较短的平均信息传播路径，从而导致其消息传播速度远快于传统媒体。根据最新统计研究，Facebook 和米兰大学公布了共同研究结果，以 Facebook 上的 721 000 000 用户数据为基础，通过统计分析，发现每两个用户之间平均通过 4.74 个间接人就能够建立联系[7]。这说明网络社交让人与人之间的联系更加紧密，原有的六度分离空间现在已经不足五度。

互联网在信息发布的速度方面具有传统媒体不具有的快速优势，是百姓了解社会动态的重要渠道。微博等互联网应用正在逐步改变社会生活方式，也在一些社会危机中表现出积极作用。在“7·23”动车事故中，微博的积极作用就得到了一次充分的展现。从 2011 年 7 月 23 日晚第一条撞车消息微博发布，到后续救援、志愿者组织、无偿献血组织、寻人等各类微博消息不断发布，微博在救援过程中发挥了重要作用。这一过程是纯粹自发行为，虽然存在信息不准确、缺乏统一协调等问题，但也让我们看到了微博在危机应对中的重要作用和价值。

但由于虚拟社会行为仍缺乏有效的监管，个别人的不负责任行为可能给其他人、其他机构、甚至整个社会带来严重伤害。若是被一些别有用心的人或组织利用，则危害更为严重。且不评论事件本身的对与错，国际上近年来发生的几次比较重大的社会群体事件，均与互联网有关，也充分展现了互联网在舆论方面的能力和价值。2011 年发生的“伦敦骚乱”、“占领华尔街”等活动的组织者主要利用 Twitter 和 Facebook 煽动和组织相关人员。2009 年在伊朗发生的“绿色革命”，Twitter、Facebook、YouTube 等互联网工具更是起到了重要的推波助澜的作用。

面对互联网舆论传播呈现出的新态势、新特点，为确保虚拟社会稳定有序的发展，避免因虚拟社会的一些谣言、非法言论造成对现实社会的伤害，我们应加强虚拟社会舆论态势的分析与监管工作：

（1）加强重大事件的分析预警能力建

设。应对相关事件的关键就在于及时发现，及时响应，以遏制其进一步扩散。应加强对重点网络平台和网络应用的分析与监管，重点解决热点问题的及时发现、跟踪，事件态势的分析与掌控等问题，提高对重大事件的预警能力，以便将一些不良势头遏制在萌芽状态。

(2)完善信息发布机制，加强舆论引导。在重大事件或群体活动中，应根据舆论发展态势，快速、准确地发布相关信息，积极引导舆论导向，掌握舆论的主动权。应重点解决热点事件的传播态势分析、舆论热点分析、舆论引导与决策、热点应用主动引导等问题，针对互联网中的各种交流平台，形成一套舆论分析与引导平台，提高对虚拟社会的舆论掌控能力。

5 网络空间安全保障

虚拟社会具有很强的技术性特点，信息网络是虚拟社会活动的载体，网络空间的安全是确保虚拟社会平稳、有序发展的关键，也是保护虚拟社会中用户隐私、用户利益的关键。据统计2011年上半年，受到过病毒或木马攻击的网民达到2.17亿，比例为44.7%；有过账号或密码被盗经历的网民达到1.21亿，占24.9%[8]。

网络空间的安全也受到各国的广泛关注，一些国家已经将网络空间安全提升至国家战略、国家安全的高度。2011年5月，美国首份《网络空间国际战略》，阐述美国“在日益以网络相联的世界如何建立繁荣、增进安全和保护开放”。这是美国第一次把其国际政策目标与互联网政策结合在一起，将此项努力与二战后建立经济和军事安全的全球框架相提并论，将外交、军事和网络安全议题进行了整合。在具体措施上，各国纷纷从技术、管理、产业、基础设施等多方面努力，加强自身网络空间安全保障能力建设。2010年，美国启动“爱因斯坦3.0”计划，加强对互联网的监管。2010年9月，美国国土安全部、国防部等政府机构组织完成了“网络风暴III”大规模网络攻防演习，这次演习中，除了美国政府机构外，还有众多大型企业和英国、瑞士等盟国的共同参与。该演习检验了美国网络空间抵御大规模攻击能力和各类典型大规模攻击的应急响应能力。另外，美国还从法律、标准规范、支撑机构等方面建立了相应的管理技术体系，比如美国国家标准技术研究所长期从事信息安全技术标准和管理规范的制定工作，起草的SP 800系列、FIPS系列标准不仅成为美国信息安全管理的重要基础，也成为世界各国的重要参考和借鉴。

我国也长期重视网络空间的安全保障工作，在法律法规、技术标准、支撑机构、产业能力等方面取得了长足的进步。在法律法规和技术标准方面，出台了《中华人民共和国计算机信息系统安全保护条例》、《计算机病毒防治管理办法》、《信息安全等级保护管理办法》等法规，信息安全产品技术标准体系也已基本形成。在支撑机构方面，建立了国家计算机网络应急技术处理协调中心、中国信息安全测评中心、信息安全等级保护评估中心等机构，从网络空间安全监测、应急响应、安全漏洞发布、安全测评等方面，构建了较为完善的安全保障技术体系。

网络空间迅速膨胀，网络攻击呈现出大规模、协同化、高危害等特点，现有的安全保障技术、管理手段仍难于满足网络空间安全保障的需要。结合我国的网络空间发展趋势，技术产业能力，以及现有的网络空间安全管理体系，建议从以下几方面加强网络空间安全保障能力，以确保虚拟社会稳定、有序发展：

(1)加强网络空间安全事件预警与应急响应能力建设。建立网络空间安全监测基础平台，以提高大规模蠕虫、分布式拒绝服务攻击、大规模僵尸网络等大规模安全事件的预警能力，进一步完善应急响应支撑体系，从应急响应队伍、应急支撑平台、应急响应预案等方面，提升大规模安全事件的应急响应能力。

(2)加强网络空间软件产品的安全评测。软件被称为信息系统的灵魂，软件安全问题是目前

网络空间安全的关键。现有的各类安全问题中，基本都与软件设计缺陷、软件有意引入恶意行为等因素有关。应针对软件安全问题从技术标准、测评体系等方面建立一套管理体系。特别是针对互联网中各类软件产品研发自由、软件规模差异大的特点，应建立面向公众的、公益性的软件安全检测服务，以提高用户对软件产品的主动检测意识；对于大规模、核心应用软件，应根据软件的不同类型实施不同层度的安全强度检测与准入制度。

（3）加强用户安全意识教育和基础安全服务能力建设。提高网络空间中每个终端的安全性是保障网络空间安全的关键，一方面，应加强用户安全意识教育，提高各用户在参与虚拟社会活动中的安全自我保护能力；另一方面，应从安全标准、安全指南等技术规范的制定，漏洞信息发布、恶意代码监测等基础服务设施的建设等方面建立面向社会大众的基础安全服务体系，为用户提供专业、有效的安全指导。

6 总结及展望

近年来网络空间的快速膨胀与渗透，使得虚拟社会已与现实社会紧密结合。虚拟社会的管理既是确保虚拟社会自身稳定、有序发展的基础，也是维护现实社会稳定和秩序的需要。

虚拟社会具有开放性、匿名性、高技术等特点，针对虚拟社会的管理问题，在借鉴现实社会管理经验的基础上，应考虑到虚拟社会的特殊性，特别是其高技术背景的特点，形成一套有针对性的管理体系。在技术支撑能力方面，应从虚拟社会管理的角度，建立一系列的支撑性技术平台，虚拟社会的管理是一个技术性很强的工作，必须有相应的技术手段支撑，依靠传统的管理手段是无法满足互联网和虚拟社会发展需要的，应该规划建立系列的技术支撑平台；在管理体系方面，应从法律法规、标准规范、机构职能等各个层面为虚拟社会的管理工作建立完善的管理体系，使虚拟社会的管理做到合法、合理、有序；在用户意识方面，应加强虚拟用户的法律意识、安全意识教育，提高虚拟社会参与者的自我保护能力和参与虚拟社会活动的责任意识。

主要参考文献

1 National Strategy for Trusted Identities in Cyberspace. 下载日期：2011年12月22日.下载地址：http://www.whitehouse.gov/sites/default/files/rss_viewer /NSTICstrategy_041511.pdf.

2 中国互联网络发展状况统计报告. 下载日期：2011年12月22日.下载地址：http://www.cnnic.org.cn/dtygg/dtgg/201107/W020110719521725234632.pdf.

3 Global Phishing Survey: Trends and Domain Name Use in 1H2011.下载日期：2011年12月22日.下载地址：http://www.antiphishing.org/reports/ APWG_GlobalPhishing Survey_1H2011.pdf.

4 Convention on Cybercrime, http://conventions.coe.int/Treaty/EN/Treaties/ Html/185.htm.

5 Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems. 下载日期：2011年12月22日.下载地址： http://conventions.coe.int/Treaty/EN/Treaties/html/189.htm.

6《中国互联网状况》白皮书.下载日期：2011年12月22日.下载地址：http://www.scio.gov.cn/zxbd /wz/201006/t660625.htm.

7 Gyarmati L, Trinh TA. Measuring User Behavior in Online Social Networks. IEEE Network Magazine, Special Issue on Online Social Networks, 2010, 24(5):26-31.

8 国家计算机网络应急处理协调中心. 2010年中国互联网网络安全报告. 下载日期：2011年12月10日. 下载地址：http://www.cert.org.cn/articles/docs/common/2011042225342.shtml.

（转至8页）

tion of two driven forces (internal and external). One conclusion of the research is that the two forces restrict each other, compromise and finally achieve a balance to determine the ideal social behaviour selection schema. The paper draws the other conclusion: the probability of the internal and external forces is identically equal to 1. For the statistically sense, the Poisson Distribution can be used as a mathematical tool to judge the gap between ideal and real social behaviour selection. The standard of the ideal social behaviour selection is just the result of the equal 0.5 of two driven forces selection probability.

Keywords network social management, social behaviour selection, social physics

牛文元 中科院科技政策与管理科学所顾问、研究员。1939年出生。中科院可持续发展战略研究组组长、首席科学家;中科院自然与社会交叉科学中心学术委员会主任;发展中国家科学院院士;《中国发展》杂志编委会主任;国家规划专家委员会委员;国家环境咨询委员会委员;国务院应急管理中心专家组成员;美国耶鲁大学SDLP讲席教授;美国弗吉尼亚大学Fulbright教授;国务院参事;第九、第十、第十一届全国政协委员。2005年被授予中国环保大使;2006年获中国绿色文明特别奖;2007年与意大利前总统钱皮一道,分获"国际圣弗朗西斯环境大奖";2007年被评为全国"10大科技英才"。E-mail:wyniu@yahoo.com

(接23页)

Challenges and Countermeasures for Virtual society Management

Feng Dengguo Su Purui

(Institute of Software, CAS 100190 Beijing)

Abstract The virtual society has closely integrated with the real world. Virtual society management is not only the foundation to ensure its stable and orderly development, but also to maintain the real world in perfect harmony. Virtual society is an open, anonymous, and high-tech community, and it has brought forward many challenges in the virtual identity management, cyber crime control, and public opinion supervision. To solve these problems, we should improve the virtual society management in technical support platform, technical standards and laws, and construct the virtual society management infrastructure.

Keywords virtual society, social management, information security

冯登国 中科院软件所研究员、博士生导师。长期从事信息安全研究工作,担任《科学通报》、*J. Comp.Sci.& Tech.*等多种杂志的编委会委员和国际信息与通信安全会议(ICICS)、国际密码学和网络安全学术会议等多个国际会议的程序委员会委员。第一、二、三届国家信息化专家咨询委员会委员,国家"十五"863计划信息安全技术主题专家组首席科学家,国家"十一五"863计划信息技术领域专家组成员。发表学术论文300余篇,出版著作30余部;获国家发明专利10余项;获国家科技进步奖二等奖3项、省部级科技进步奖一等奖6项;曾获中科院十大杰出青年、国家重点实验室计划先进个人、中科院青年科学家奖、首届全国优秀博士学位论文奖等多项荣誉;国家杰出青年科学基金获得者和中科院"百人计划"入选者。E-mail:fengdg@263.net