新一代互联网安全管理体系研究框架：阳光互联网倡议

唐鑫[1]，吴晓松[1]，黄伟[1]，LEE Jae Kyu[1,2]，赵玺[1]，王嘉寅[1]
1. 西安交通大学管理学院，陕西 西安 710049；2. 韩国科学与技术研究院，韩国 大田 34141

摘要
传统的互联网已经成为全球范围内匿名用户网络犯罪、网络欺诈和恐怖主义的雷区。为了从根本上解决网络安全问题，世界信息系统协会制定了一个基于信息通信技术和大数据技术的阳光互联网宏伟倡议，为传统的网络安全框架提供了一种全新的研究框架，在适当的层面保护用户隐私。基于阳光互联网的5项原则和中国网络安全现状，提出3点可实现的安全架构途径。

关键词
网络犯罪；大数据；阳光互联网；用户隐私

中图分类号：TP393 文献标识码：A doi: 10.11959/j.issn.2096-0271.2018007

Framework of next-generation internet security management: bright internet initiative

TANG Xin[1], WU Xiaosong[1], HUANG Wei[1], LEE Jae Kyu[1,2], ZHAO Xi[1], WANG Jiayin[1]
1. School of Management, Xi'an Jiaotong University, Xi'an 710049, China
2. Korea Advanced Institute of Science and Technology, Daejeon 34141, Republic of Korea

Abstract
The internet has become a minefield of crime, fakes, and terrors perpetuated by anonymous users on a global scale. In order to fundamentally solve the problem of cyber security, the Association for Information Systems (AIS) has developed a grand initiative for the bright internet based on information and communication technology and big data technology. The proposed initiative not only provides a new research framework for the traditional cyber security framework, but also protects user privacy at an appropriate level. Based on the five principles of bright internet and the data of Chinese cyber security, three approaches were proposed to achieve security architecture.

Key words
cybercrime, big data, bright internet, user privacy

1 引言

近年来，网络信息系统正日益受到网络犯罪、网络攻击以及隐私侵犯等不安全行为的影响。2016年，美国Verizon无线公司的数据显示：每年有超过37亿的互联网用户遭受网络犯罪的攻击，其中38%是移动客户端用户，直接造成的经济损失高达4 000亿美元；每天网络上平均新增超过560亿封垃圾邮件；超过71%的网站存在时间不超过24 h；60%的美国公司曾遭受分布式拒绝服务（distributed denial of service，DDoS）攻击，这些潜在的网络攻击甚至会对社会基础设施造成严重破坏，直接影响国家的财政、金融、交通、通信等正常工作。与此同时，侵犯个人隐私的事件也在网络中屡禁不止。统计数据显示，每年有超过55亿条用户信息被窃取。网络上不仅存在个人隐私信息泄露的问题，网络欺凌、网络暴力等违法犯罪行为也正严重危害着社会的法制文明建设。

传统的企业安全系统不仅需要花费巨额的资金进行部署与维护，而且容易遭受网络不法分子的攻击。为了解决互联网上存在的安全问题，韩国Lee Jae Kyu教授提出了基于信息通信技术与大数据技术的一种全新互联网安全架构——阳光互联网（bright internet）架构。这一全新的架构不仅可以解决网络上存在的网络犯罪、网络攻击等非法行为，而且可以保障网络用户的信息不受侵犯，防止青少年沉迷网络、遭受网络欺凌和网络语言暴力的攻击。

2 阳光互联网的5项原则

传统网络安全防护架构难以取得显著成效，其原因主要有3个：匿名式的攻击、被动式的防御和局部式的治理。

（1）匿名式的攻击

既有的TCP/IP为了保障每个网民在网络中的隐私以及言论表达自由，实行的是可匿名的网络接入，但这同时也成了网络安全威胁难以被根治的本质原因。大多数的网络攻击、网络诈骗、网络犯罪都是匿名式的攻击，攻击者隐藏自己的真实身份或者通过僵尸机发动目的性的网络攻击，攻击方与被攻击方之间的信息不对称，往往导致被攻击方难以有效识别攻击者，处于被动地位，继而难以实施有效的反击手段。匿名式的攻击实际上造成了攻击方相对被攻击方天然的优势，俗称“敌暗我明”，这也导致了当前网络安全防护的第二个弊端——被动式的防御。

（2）被动式的防御

网络的匿名机制使人们不能有效地预防网络攻击，而只能通过各种安全防护手段被动地进行防御。当前主要的网络安全防护仍是采用企业层面传统的防火墙、杀病毒、入侵检测等被动式的防御系统和治理措施，被动地“封堵查杀”，不能从根本上解决新出现的各种攻击行为，难以解决网络安全问题。在现实生活中，有违法必究的社会法制，受害者能通过诉诸法律来维护自身的权益，并可以依法对犯罪分子进行追责和惩处，而在网络世界里，却没有相应的追踪、惩处机制。网络罪犯往往可以逍遥法外，受害者却难以维护自身正当的权益，无法让网络罪犯付出应有的代价，而这正是“网络罪犯猖獗”的重要原因。

（3）局部式的治理

目前的网络安全治理模式主要是以企业为单位或者以国家为单位的局部式治理，而这与网络安全问题的全局性以及全球性相矛盾。以企业为单位的安全防护方案会给企业本身带来高昂的成本，同时，每

个企业独立部署相同的安全方案也会造成极大的社会资源浪费，需要强调的是，基于企业利益的安全治理方法不能保证同时实现个体隐私安全。以国家为单位但缺乏国际间协作的安全防治方案，一方面，难以对国际网络犯罪行为进行追踪和惩处，另一方面，社会公众的网络安全保障与个体公民的隐私安全存在矛盾，如斯诺登曝光的美国“棱镜计划”。如何通过系统设计，从全局整体的角度构建新的网络安全防护架构，从而实现对当前网络安全威胁的有效预防与根治，将是人工智能时代的网络安全防护架构需要重点思考和解决的问题。

基于此，Lee Jae Kyu教授提出了构建阳光互联网安全架构的5项基本原则[1]：源头问责、传播者问责、可识别的匿名、全球协作搜索以及隐私保护。

2.1 源头问责

源头问责指恶意代码和非法窃听的网络攻击发起者都应该为他们的恶意行为以及产生的后果负责，因此，攻击源的IP地址需要可追踪。这一原则的内涵是即使在网络世界里，每个人也需要为自己的行为负责。

以垃圾邮件为例，源头问责原则要求在源服务器上对传出的邮件进行监控。在传统的网络安全架构下，源服务器对于垃圾邮件的发出并没有任何责任，导致源服务器提供商没有足够的动力对这些邮件进行安全性排查，也无从对垃圾邮件发出者进行有效的问责。而一旦要求对垃圾邮件发出者进行问责，在垃圾邮件发出者发送邮件给源服务器时，就会被实时识别，拒绝发送，从而在源头上解决攻击的产生。

可见，源头问责原则意味着恶意代码和黑客攻击的起源者、起始IP地址都可以被追踪[2]，这与国际网络安全责任原则基本相同。源头问责原则可以被运用到个人用户、服务器、企业和国家层面。但是对于恶意的国家主导的网络攻击（state-led cyber attack，SLCA）来说，主导的国家有可能刻意隐瞒攻击源头，这种源头不明的恶意攻击责任应该由主导的国家承担。此外，恶意的攻击行为可能使用其他国家的计算资源，导致追踪恶意攻击源头时，将其他国家误认为恶意攻击的发起国。因此除了源头问责，需要建立第二条基本原则——传播者问责。

2.2 传播者问责

传播者问责是指僵尸机、网络服务提供商等各种网络分发源都有责任相互协作，共同阻止可识别的网络攻击。无论这些分发源是有意还是无意，只要参与了网络攻击的传递和分发，就应该被追究相应的责任。长效的网络安全防护机制需要让每一个用户（个体、企业、国家）从被保护者变成网络安全的建设者。虽然源头问责原则可以显著减少垃圾邮件，但90%的垃圾邮件都是由受攻击的计算机发出的，DDoS攻击是由数以百万计的僵尸电脑造成的，电信运营商也是在不知道内容和后续有害影响的情况下，提供短信和语音网络钓鱼。因此，建议对发送者进行匿名监控，以防止有害信息的传递。

传播者问责原则意味着即使遭受网络攻击的计算机或互联网服务提供商无意间感染僵尸电脑传播的病毒，也应第一时间报告其状态，以防止这些感染的电脑再次向其他用户传递可识别的伤害[3]。传播者问责需要各种网络服务中介承担起应有的传播责任。

2.3 可识别的匿名

为了保证言论自由，必须允许网络匿名。然而，网络罪犯几乎总躲在匿名的背后。当黑客攻击索尼公司时，警方无法迅速追踪到黑客的原始服务器，因为互联网协议无法有效地追踪来源和真实姓名。因此，当网络犯罪被发现时，数字搜索授权应该立即授权追踪攻击来源[4]和黑客的真实姓名，以防止匿名的滥用。Ahn L V等人[5]研究了有选择性的匿名性技术，然而相关功能实现需要法律允许在检测到犯罪时跟踪真实姓名。

韩国宪法法院裁定，要求大型门户网站公开用户真实姓名的法律是违宪的，因为该法律违反了宪法规定的言论自由[3]。然而，这一判决并不是允许互联网上存在匿名犯罪行为，两种匿名性需要区别开来：言论自由和防止匿名犯罪。在言论自由的层面上，公民的匿名性应该受到保护。一旦发现了违法行为，匿名用户的真实姓名应该是可追踪的[6]。为了保护国家安全并且解决网络犯罪问题，采用可识别的匿名原则是必要的。

确定适当的匿名性和安全性是一个有争议的问题。只有当用户犯罪时才允许跟踪，即在检测到用户犯罪时激活相应的数字搜查令。将可追溯性与基于规则的数字搜索令结合起来，以保护国家安全和用户隐私安全。

即使在网吧和无线网络这样的公共访问区域，也需要设计一些方案来保证用户真实姓名的可追溯性。如果不确定用户的真实姓名，访问服务提供者应在发生非法活动时承担责任。这样，服务提供者会谨慎对待访问其网络的潜在有害行为，2013年9月1日起我国施行的《电话用户真实身份信息登记规定》就是该原则最真实的写照。

即使可以识别源IP地址，恶意攻击者也会使用假名隐藏真实姓名。因此，可识别的匿名原则是必要的，这意味着当匿名攻击发生时，攻击来源的真实姓名或等同身份应该在有效搜索令的请求下实时识别，而那些无辜的网民可以持续匿名[2]。目前，一些方法可以用来实现可识别匿名的原则，但是一些网络恐怖主义国家不会遵守这一原则，这就需要制定政策和技术，以实现可追踪的匿名性。如果犯罪源自另一个国家，跨境合作也是必要的。全球各国政府应该合作，以防止网络犯罪天堂的出现。

2.4 全球协作搜索

为了在全球范围内实施阳光互联网的原则，互联网用户国家之间在沟通、合作、执行和报告方面的全球协作至关重要[2]。通过协同搜索，可以确定全球范围内攻击者的真实姓名。但是，网络恐怖主义国家不会参与这样的合作。阳光互联网安全架构原则强调构建国家间的国际合作是一项基本原则，是源头问责原则、传播者问责原则以及可识别的匿名原则有效实施的保障。

及时调查国家主导的网络攻击需要有效的国际调查合作。然而，由于技术和政治原因，国际调查合作并不容易达成。2007年4月发生在爱沙尼亚的网络战被视为第一场国家层次间的网络战争，俄罗斯拒绝2007年爱沙尼亚提出的联合调查。此外，每个国家的不同法律制度都可能会拖延调查。2000年，来自菲律宾的病毒“I Love You”通过电子邮件传播到全球，直接造成87亿美元的经济损失，但由于菲律宾没有相应的法律，无法起诉[7]。制定协作搜索的全球法律标准框架对于防止来自第三国的迂回网络攻击至关

重要。但是，防止那些不加入阳光互联网计划的非成员国的袭击需要额外的威慑措施。

2.5 隐私保护

预防安全原则的一个基本前提是不侵犯无辜网民的隐私，因此，阳光互联网架构不仅要在技术上对隐私保护给予支持，而且应该在法律上完善设计[2]。

通过区分无辜网民、恶意犯罪分子以及恐怖分子，可以保障互联网上无辜网民的隐私不受侵害。为了保护无辜网民的隐私，必须由信任的第三方进行透明的审核，因此禁止非法登录访问私人数据的隐私保护技术将是必要的[8]。为了实现可识别的匿名而存储真实姓名时，可以使用适当的加密算法，使得在没有有效搜索令的情况下私人信息不会被泄漏。但是，非阳光互联网成员国网民的隐私无法得到有效防护，从而吸引尽可能多的国家加入阳光互联网中。

3 大数据背景下互联网安全问题

2016年是我国网络安全重要发展的一年。2016年4月19日，习近平总书记在网络安全和信息化工作座谈会上指出：我国应该推进网络强国建设，让互联网更好地造福国家和人民。2016年11月7日，在全国人民代表大会常务委员会第二十四次会议上通过了《中华人民共和国网络安全法》，并于2017年6月1日正式实施。法律的颁布保障了我国公民在互联网上的合法权益不受侵害，维护网络空间安全和社会公共利益安全。2016年12月27日，国家互联网信息办公室发布了《国家网络空间安全战略》。法律与战略的颁布从根本上维护了国家在网络空间的主权与安全，为实现我国网络强国战略保驾护航。

根据《中国网民权益保护调查报告2016》显示，2016年我国网民因为隐私泄露造成的损失高达915亿元，超过84%的网民受到隐私泄露的不良影响。根据12321网络不良与垃圾信息举报受理中心的统计显示，2016年12月，涉嫌诈骗电话有效举报9 322件，其中，金融类诈骗占42.8%。短信诈骗举报3 384件，网购类诈骗占37%，中奖类诈骗占35.2%。随着数字化技术的发展，公民信息泄露已呈现高发趋势，形成巨大的黑色产业链。拥有大量个人信息的企业成为隐私泄露的主要来源，接近一半的严重的网络经济犯罪事件都是由内部人员造成的。然而，企业在新的业务过程和技术实施中并没有过多关注隐私。为了更好地保护公民隐私权利，有效减少隐私泄露带来的损失，需要明确企业在保护公民隐私方面的责任。

3.1 木马和僵尸网络病毒

2016年，大约96 670万个木马和僵尸网络病毒控制端控制了中国境内1 700多万台主机，而2015年大约有105 056万个木马和僵尸网络病毒控制端控制了中国境内的1 462万余台主机。木马和僵尸网络病毒控制端主要来自于美国、欧洲与中国台湾地区。其中，美国控制中国境内大约475万台主机，欧洲与中国台湾地区控制大约335万台主机。控制主机规模为100台的僵尸网络集群约为4 896个，控制主机规模在10万台以上的僵尸网络集群约为52个。

2016年中国木马和僵尸网络受控主机数量地区分布情况如**图1**所示。可以看出，我国境内感染木马和僵尸网络病毒的地区

主要分布在沿海与发达的省会城市。从主机感染数量来看，前5名的地区分别是广东省、江苏省、山东省、浙江省、河南省，这5个地区受感染的主机约占全国感染木马与僵尸网络病毒的主机数量的一半。

3.2 移动互联网恶意程序

根据国家互联网应急中心提供的数据，2016年网络上捕获的移动互联网恶意应用程序（App）多达2 053 501个，较2015年的1 477 450个增长了39%。**图2**是2005—2016年移动互联网恶意程序增长走势，可以看出2005—2010年增长率基本持平，2010—2016年则保持高速的增长。从**图3**可以看出，在2016年捕获的互联网恶意程序中，流氓行为类程序、恶意扣费类程序以及资费消耗类程序比例占据前3名，分别为61.1%、18.2%和13.6%。移动互联网恶意程序下载链接接近67万条，较2015年的30万条增长近1.2倍，涉及的传播源域名22万余个、IP地址3万余个，恶意程序传播次数高达1.24亿次。

目前，移动互联网应用程序是恶意程序传播的载体，其传播方式与传播途径多种多样，包括App商店、云端、云盘、广告平台等。2016年，在公安机关备案的141个应用商店数据显示，恶意App传播事件高达8 910起，同比2015年下降47.8%。其中，国内领先的企业级云服务商七牛云通报恶意App事件1 413起，腾讯网通报恶意App传播事件1 223起，其他网站或App商店（如百度、悠悠村、安智网等）都发现了恶意App传播事件。报告显示，移动互联网恶意程序持续快速增长，在此条件下恶意App在正规应用商店中下载传播得到有效的控制，但通过非正式的应用商店下载传播的恶意程序的数量还在不断增长。

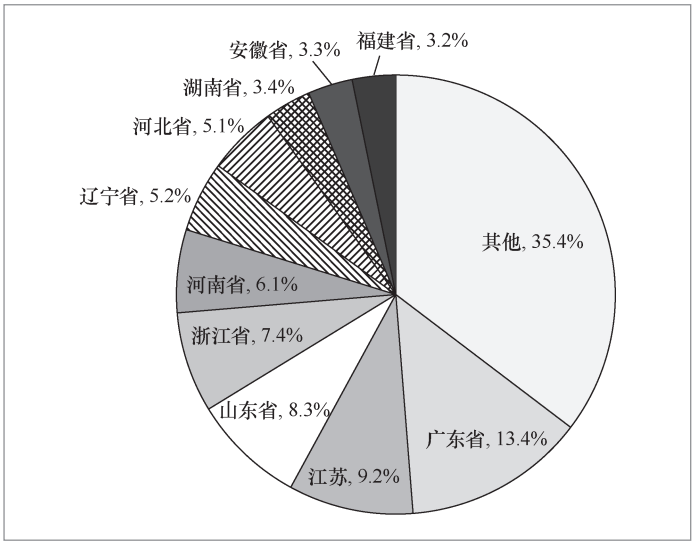

图 1 2016 年中国木马或僵尸网络病毒受控主机数量地区分布

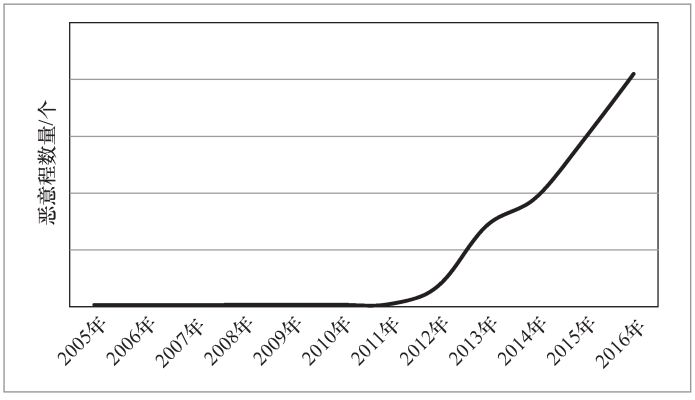

图 2 2005—2016 年移动互联网恶意程序增长走势

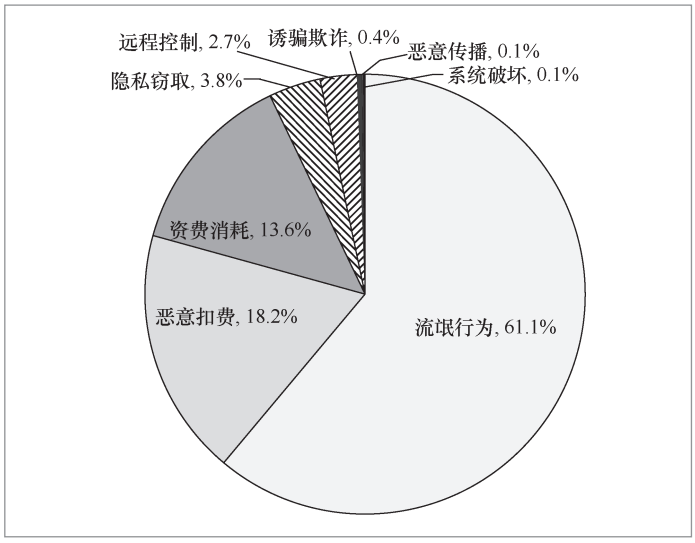

图 3 2016 年移动互联网恶意程序比例

3.3 DDoS攻击

2016年，国家互联网应急中心组织许多通信行业和安防行业单位，宣布成立中国互联网网络安全威胁治理联盟。该联盟着力解决网络安全威胁，力争开展DDoS防范打击协同治理，有效缓解了DDoS攻击的危害，2016年超过1 Gbit/s的DDoS攻击次数日均达452次，比2015年下降了60个百分点。但是，大流量攻击事件大幅增长，2016年第一季度平均每日10 Gbit/s以上的攻击次数增加了四分之一，平均每天133次，占日均攻击的29.4%。每日超过100 Gbit/s的攻击次数平均达到6次以上，此外，云平台还多次遭受500 Gbit/s的攻击。从恶意攻击的目的来看，67%涉及互联网地下黑色产业链；从恶意攻击方式来看，反射攻击仍然是主流；从恶意攻击源IP地址对应的设备来看，除了传统的PC端和数据中心服务器，智能设备越来越多地被用作DDoS攻击工具。

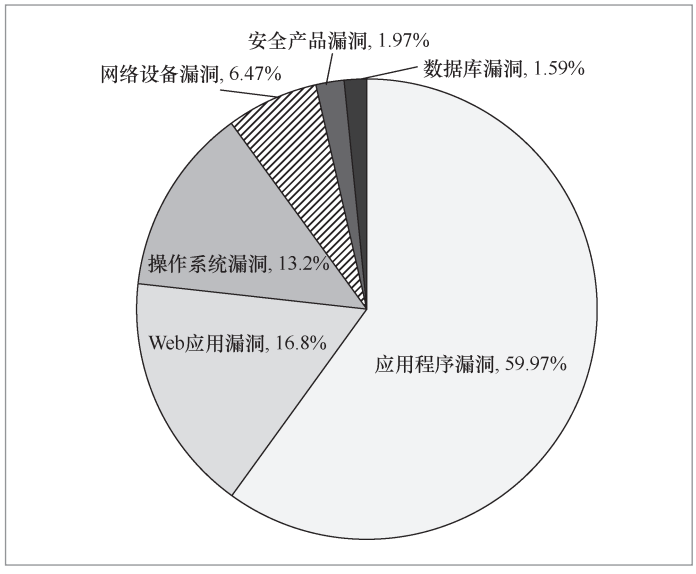

图 4 2016 年国家信息安全漏洞共享平台收录的漏洞类型占比

3.4 安全漏洞

2016年，国家信息安全漏洞共享平台收录了10 822个漏洞，比2015年增长33.9%，其中，高风险漏洞4 146个，比2015年增长29.8%。此外，2016年的“零日漏洞”约为32 203个，比2015年增长82.5%。从**图4**可以看出，应用程序漏洞占59.97%，Web应用漏洞占16.8%，操作系统漏洞占13.2%，网络设备漏洞占6.47%，安全产品漏洞占1.97%，数据库漏洞占1.59%。2016年，国家信息安全漏洞共享平台加强了一般硬件和软件漏洞的原始收集工作，成为全年新增增长点，全年接受国内漏洞报告平台与安全厂商提交相关的漏洞总数为1 926个，占总提交漏洞数的17.8%。

国家信息安全漏洞共享平台对存在的漏洞进一步完善，建立了移动互联网、电信行业、电子政务和工业控制系统4种子漏洞数据库，收录漏洞的数量分别为98个、640个、344个和172个，占全年收录漏洞数量的比例分别为9.1%、5.9%、3.1%和1.5%。对重点关注的子漏洞数据库安全漏洞影响情况进行检查可知，涉及政府机构的年度报告、重要信息系统部门和行业安全的漏洞高达24 246个，较2015年上升3.1%。

3.5 网站安全

2016年，互联网上仿冒我国网站网页约有178 000个，较2015年下降了3.6个百分点。对IP地址进行追踪发现，大约20 000个IP地址承载了上述的仿冒网站，其中境外的IP地址占有率达到了85.4%。此外，大约40 000个IP地址对我国超过820万个网站植入后门，较2015年增加了

9.3%。我国境内的17万个网站遭到篡改，较2015年下降了31.7%，其中有467个政府网站被篡改，较2015年下降了47.9%。从篡改的方式来看，通过植入非法链接的方式篡改的网站占86%，植入非法链接是中国境内网站被篡改的主要方式。从篡改类型分布来看，以.com作为后缀的商业网站被篡改得最多，占总数的72.3%，以.net为后缀的网络服务公司和以.gov为后缀的政府网址分别占据总数的7.3%和2.8%。

4 基于中国互联网实情的阳光互联网安全架构可实现途径

近年来，随着中国法律法规和网络安全管理体系的不断完善，网络安全技术在我国电力资源、人才队伍以及国际合作等方面取得了明显成效。我国互联网安全整体形势趋于稳定，网络安全保护能力迅速提升，网络安全国际合作进一步加强。随着网络空间战略地位的不断提高，世界主要国家的网络空间攻击能力不断提升，随着国家之间网络安全冲突日益增多，中国网络空间安全也面临着复杂的挑战。结合中国网络安全的实际情况，并基于阳光互联网的5项原则，提出3点可实现的安全架构途径。

4.1 “隐私保护—安全防控”双层架构

互联网安全专家指出，在犯罪行为发生前就进行监测可以及时制止犯罪行为的发生或者在犯罪行为发生后能实时追踪。但是，在犯罪行为发生前，没有人有权利去“窥视”每个网民的行为。因此，基于阳光互联网的可识别匿名原则与隐私保护原则，设计犯罪分子行为监测预警与合法网民隐私安全保护的均衡机制，以解决“匿名式攻击”的弊端。阳光互联网不再是单一的匿名层架构，而是包含了“隐私保护层”和“安全防控层”的双层架构。在隐私保护层网络用户都是匿名的，而在安全防控层可以实现所有用户的实名，正常的网络运行架构是隐私保护层，一旦产生了网络犯罪行为，相关的网络安全执法部门可以向国际/国家相关机构申请授予数字搜查令，从而进入安全防控层对该网络犯罪行为进行实名搜索，获取安全防控层对该违法犯罪行为的所有监测资料，作为后续起诉的依据。而这个过程中不会对其他用户的隐私造成侵犯，实现了无辜网民隐私防护与网络罪犯实名查处的双赢。“隐私保护—安全防控”双层架构是专门为解决这一问题而设计的，可以通过人工智能技术监测网络所有用户的行为，只有发现可疑行为并预警时，人们才可以通过数字搜查令对相关犯罪分子进行实名跟踪，并获取关于该犯罪分子之前的所有监测数据。在技术层面，构建技术合作可以推动这一双层架构的实现。在政策层面，为了保证网络实名层的有效实现，需要出台一定的措施保障实名入网的推行，比如，某咖啡店没有保证连接其Wi-Fi网络的所有用户实名，一旦该网络下的用户实施了违法行为，这家咖啡店就必须承担责任。

4.2 “主动式追踪”网络犯罪分子架构

基于阳光互联网的“可识别的匿名原则”与“全球协作搜索原则”，构建主动追踪式的网络安全治理模式，进而破除“被动式防御”的弊端。如图5所示，当中国需要跨国追踪国外网络犯罪分子时，只需向“阳光互联网安全管理架构国际中心”申请“国际数字搜查令”，国际

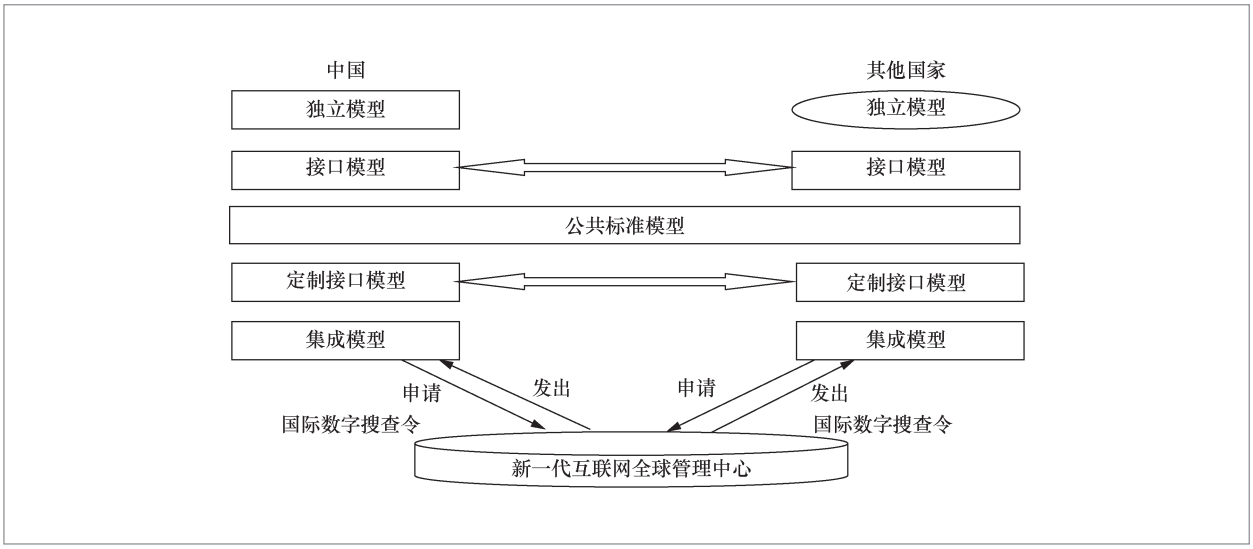

图 5 “主动式追踪”网络犯罪分子架构

管理中心评估核实之后就会向相应国家发出“国际数字搜查令”，然后由该国实施实名追踪和抓捕，通过全球协作搜索原则，可以实现不侵犯他国网络空间主权的同时对跨国网络罪犯实施抓捕。在技术实现层面，只要通过“隐私保护—安全防控”双层架构获取犯罪分子的真实身份信息，即可通过线下安全执法部门实施抓捕。在国家政策层面，应该出台政策成立相应的执法部门，制定相应的抓捕程序。在国际协作层面，需要成立专职的“阳光互联网全球管理机构”推动这一协作的达成，而相应的国际抓捕程序也需要加以制定。

4.3 “全局式治理”的网络安全问责架构

应基于阳光互联网的源头问责原则、传播者问责原则以及全球协作搜索原则，构建全球范围内的网络安全问责架构，从而破除局部式治理的弊端。如图6所示，首先，源头问责原则要求对网络攻击发起方、网络犯罪分子进行责任追究和惩处，这是网络安全问责层次结构的核心，而主动式追踪则构成这一问责层次有效实施的基础。其次，传播者问责原则要求对发布病毒软件、诈骗信息的网络代理商进行问责，这是网络安全问责层次结构的重要部分。邮件系统代理商分发垃圾邮件、商业诈骗邮件，要追究其相应责任，被黑的服务器攻击无辜网民或者企业政府，黑客本身自然要基于第一问责层次进行惩处，但是被黑服务器的拥有方也需要承担相应的责任。最后，全球协作搜索原则构建了国际间网络犯罪的问责层次，信息安全公司Sophos公布的一份研究报告显示美国仍然是世界垃圾邮件的主要来源国，尽管对垃圾邮件的发出者、企业需要追究责任，但是垃圾邮件的主要产生国家也需要基于国际协议被追究相应责任，从而督促各国治理国内网络安全威胁，共同维护国际网络安全。追踪抓捕网络犯罪分子后的主要任务是量化罪责并施以惩处，而在全局治理模式下，除了攻击源（犯罪分子）需要问责，相应的分发源以及来源国也需要进行问责，因此需要构建一套“指标体

系”来对多方定责。而这一指标体系实施的可能的技术解决方案是可信计算。这种信任机制可以构建并评估网络每一个主体的信任值，对信任值低于平均值要求的网民处以一定的罚款以及刑责、企业处以一定的征税与刑责、国家处以相应的罚款与制裁。在技术实现层面，可通过与企业技术合作实现“信任指标”；在国家政策层面，需要出台针对网络罪犯处以相应罚款与刑责的制度政策；在国际协作层面，需要共同遵守问责机制。

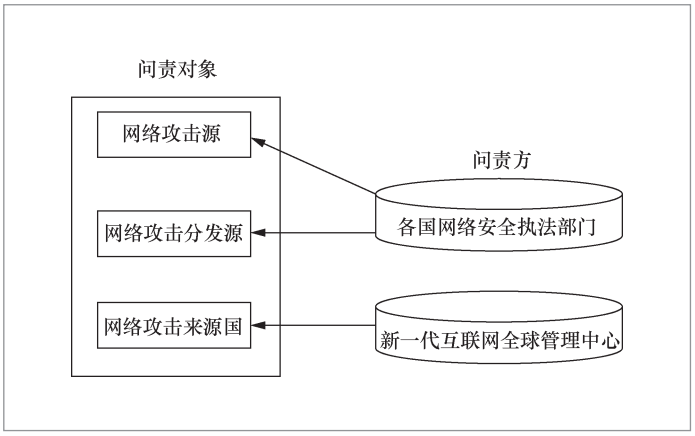

图 6 “全局式治理”的网络安全问责框架

5 结束语

网络恐怖主义和网络犯罪日益猖獗，已经造成了重大的社会和经济损失，威胁着国家安全和可持续发展的基础。然而，当前网络安全架构无法识别恶意发起人，并阻止他们进行网络攻击。因此，本文提出了阳光互联网安全管理架构，通过这一架构的5项基本原则构建了一套新的“可识别匿名、主动式追踪、全局式”的安全治理模式。这是一种预防式的安全管理范式，致力于保证无辜网民言论自由和隐私安全的同时，对网络罪犯进行有效的实时识别和预防。我国如果能充分把握这一时代机遇，将很有可能主导阳光互联网安全管理架构的全球建构，并占据充分的话语权。

参考文献:

[1] COBB C. Network security for dummies[M]. Hoboken: John Wiley & Sons, 2011.

[2] LEE J K. Research framework for AIS grand vision of the bright ICT initiative[J]. MIS Quarterly, 2015, 39(2).

[3] LEE J K. Invited commentary-reflections on ICT-enabled bright society research[J]. Information Systems Research, 2016, 27(1): 1-5.

[4] BABA T, MATSUDA S. Tracing network attacks to their sources[J]. IEEE Internet Computing, 2002, 6(2): 20-26.

[5] AHN A V, BORTZ A, HOPPER N J, et al. Selectively traceable anonymity[C]//The 6th International Conference on Privacy Enhancing Technologies, June 28-30, 2006, Cambridge, UK. Heidelberg: Springer Press, 2006, 4258: 208-222.

[6] WONDRACEK G, HOLZ T, KIRDA E, et al. A practical attack to de-anonymize social network users[C]// 2010 IEEE Symposium on Security and Privacy, May 16-19, 2010, Berleley, USA. Piscataway: IEEE Press, 2010: 223-238.

[7] DEFLEM M, SHUTT J E. Law enforcement and computer security threats and measures[M]// Global perspectives in information security: legal, social, and international issues. New York: Wiley, 2008.

[8] AGRE P E, ROTENBERG M. Technology and privacy: the new landscape[M]. Cambridge: Mit Press, 1998.

作者简介

唐鑫(1990-),男,西安交通大学管理学院信息系统与电子商务系博士生,主要研究方向为安全大数据、数据分析与数据挖掘。

吴晓松(1992-),男,西安交通大学管理学院信息系统与电子商务系博士生,主要研究方向为安全大数据、方案管理。

黄伟(1964-),男,西安交通大学管理学院教授、博士生导师、院长。教育部长江学者特聘教授,国家“千人计划”特聘专家,美国哈佛大学Fellow和美国俄亥俄大学商学院管理信息系统系终身正教授。出版学术专著10余本,在国际知名期刊和会议上发表学术论文120余篇。其研究成果被引用次数超过1 700次,H因子为22。主要研究方向包括基于新一代信息技术的管理沟通、安全大数据、群体支持系统、大数据管理与数据质量、电子政务/电子商务、IT与服务外包、IT/IS管理。

Lee Jae Kyu(1943-),男,韩国科学与技术研究院教授、阳光互联网研究中心主任,世界管理信息系统大数据领域权威学者之一,韩国科学院院士。阳光互联网原则的创立者,曾获得韩国政府颁发的国家勋章,9次获得信息系统领域知名会议最佳论文奖。主要研究方向包括人工智能在管理决策支持方面的应用,绿色IT、新一代互联网平台的创建(从技术、政策和全球管理等角度),现已获得安全领域45项相关项目的资助。

赵玺(1981-),男,西安交通大学管理学院副教授,《IEEE Transactions on Image Processing》《IEEE Transactions on System》等国际知名期刊审稿人,IEEE International Conference on Biometrics: Theory, Applications and Systems和IEEE International Conference on Automatic Face & Gesture Recognition等国际会议联合主席、技术程序委员会委员,发表学术论文40余篇。主要研究方向包括数据分析、机器学习、生物计量学、云计算、移动计算、商务智能、安全大数据。

王嘉寅(1985-),男,西安交通大学管理学院教授、博士生导师,陕西省第九批“百人计划”入选者,西安交通大学第二批“青年拔尖人才支持计划”入选者,陕西省医疗健康大数据工程研究中心副主任。美国阿肯色大学首席数据官研究院客座研究员,美国麻省理工学院斯隆管理学院国际首席数据官协会提名创始会员。发表论文30余篇,累计他引次数近500次,其中1篇论文从2015年至今一直入选基本科学指标数据库高被引论文。主要研究方向为以精准医疗大数据为背景的全面数据质量管理。

收稿日期:2017-12-11