

暗网治理思路

周琳娜 高 存

(国际关系学院信息科技学院 北京 100091)

(zhoulinna@tsinghua.edu.cn)

Train of Thought on Governance of Dark Web

Zhou Linna and Gao Cun

(School of Information Science and Technology, University of International Relations, Beijing 100091)

Abstract Internet has become an indispensable impetus to accelerate the development of human society. But what cannot be overlooked is while Internet promotes human development and progress, its unique unboundedness and anonymity have also brought many hidden dangers to global security. Dark Web, the most covert and darkest part of cyberspace, carries the worst cybercrimes. Drug, population and arms trafficking, terrorism, political subversive activities and other crimes are almost filled with the entire dark Web space, which poses a great threat to global security. Effective methods to dark Web governance is extremely urgent. Many Internet powers have taken actions to dark Web governance, but produce very little effect due to the differences in their respective purposes, methods, and even ideologies. Dark Web governance has become a common problem facing all countries. On December 16, 2015, General Secretary Xi Jinping proposed to build “a community of shared future in cyberspace” for the first time at the Second World Internet Conference, emphasizing that “Cyberspace is a common activity space for human, and the future of cyberspace should be shared by all countries in the world. Every country should strengthen communication, expand consensus, and deepen cooperation.” This undoubtedly provides a Chinese idea for dark Web governance. In the context of rapid development of globalization and with the guidance of building “a community of shared future in cyberspace”, we propose several methods and recommendations for dark Web governance.

Key words a community of shared future in cyberspace; dark Web; dark Web governance; hazards of dark Web; cyber security

摘 要 高速发展的互联网已成为促进人类社会进步不可或缺的重要力量。但不可忽视的是，互联网在促进人类发展进步的同时，其特有的无界性和匿名性也为全球安全带来了诸多隐患。暗网——网络空间中最为隐蔽、最为黑暗的部分，也承载着最为恶劣的网络犯罪行径。毒品交易、人口、

收稿日期:2018-04-19

基金项目:国家自然科学基金重点项目(U1536207);国家重点研发计划项目(2016QY08D1600);国家重点研发计划课题(2016YFB0801405)

通信作者:高存(gaocun_uir@163.com)

武器贩卖,恐怖主义,政治颠覆等犯罪行为几乎充斥着整个暗网空间,给全球安全造成了极大的威胁,暗网治理迫在眉睫。由于暗网自身具有隐匿性强、变化快、危害性大等特点,其治理的技术难度很高,在制度制定方面也存在很多问题。世界各网络大国虽然已经采取了不少措施治理暗网,但都因各自的目的、方法、手段甚至意识形态的不同,收效甚微。如何有效治理暗网,已成为一个困扰世界各国的全球难题。2015年12月16日,习近平总书记在第二届世界互联网大会上首次提出了构建“网络空间命运共同体”的设想,强调“网络空间是人类共同的活动空间,网络空间命运应由世界各国共同掌握。各国应该加强沟通、扩大共识、深化合作”,这无疑为暗网治理提供了中国思路。在全球化快速发展的背景下,以“网络空间命运共同体”的理念为指导,提出了暗网治理的方法和建议。

关键词 网络空间命运共同体;暗网;暗网危害;暗网治理;网络安全

中图法分类号 TP309

截至2017年6月1日,全球网民数已达34亿,同比增长10%,互联网全球渗透率达到46%^[1],网络空间正在成长为继陆、海、空、天后的第五空间。网络空间对人类社会发展的巨大推进力已无需赘言,然而伴随着网络发展出现的众多安全威胁也是不可忽视的。近年来,随着全球化程度的不断提高,各国也越来越清楚地认识到,作为连接全球信息桥梁的网络空间,其安全问题涉及到的领域不只有国家的经济、金融,更有国防、政治和文化。如何保障网络安全已经成为国际和国家事务中待解决的重要问题。网络安全合作在国际政治和外交议程中的重要作用日益凸显,双边网络安全合作、区域网络安全合作和多边合作也日益紧密且多元化。表面上看,世界各国对网络空间安全的治理手段是合理且有效的,但事实上,网络空间的极大部分仍处于黑暗之中。如何打破黑暗,让整个网络空间暴露在光明中,各国都有很长的路要走。暗网,作为巨大黑暗中更为漆黑的一点,其该如何治理自然成为各国政府在构建安全网络环境过程中绕不开的棘手难题。

1 暗网,威胁全球安全的毒瘤

1.1 关于暗网

在绝大多数人眼中,互联网就是那些可以用传统的搜索引擎搜索到的网站集合,其实不然,这些可以被搜索到的网站集合只是互联网中很小的一部分,也被叫作表层网^[2]。除此之外,互联网中还有很多由于各种技术原因不能被搜索引擎索引到的部分,叫作深网。在深网中还有一些被刻意隐

藏的网站,这些站点需要通过特殊的软件才可以访问,通常被定义为暗网^[3]。暗网是利用加密传输、P2P对等网络、多点中继混淆等,为用户提供匿名的互联网信息访问的一类技术手段^[4],其最突出的特点就是匿名性。用户可以在暗网中分享文件和信息,却几乎不可能被追踪到真实的身份信息,这对犯罪分子来说无疑是天堂。暗网的核心技术是洋葱路由,该技术最早由美国国防高等研究计划署和美国海军研究实验室提出,用于保护军事通信安全。洋葱路由,顾名思义就是用户在发送数据时,对数据的加密转发就像在剥洋葱。用户先选定一条路由,将要发送的数据和相关路由信息进行多层加密,之后将其发送到事先选定的中继节点中的首个节点,节点收到加密信息后就可以使用自己的特定密钥解密报文,如同剥掉一层洋葱皮,得到下一个节点的IP信息和报文数据,并将其转发给下一个节点,如此重复,直到将报文转发给目的节点。虽然每个节点的出入站信息都可以被查到,但是想要查到路由的真正起始点需要整个链路上的所有节点的出入站信息,而这几乎是不可能的。暗网的存在本身并不违法,但是其匿名性一旦被不法分子所用,就相当于为违法犯罪提供了天然的屏障,也为打击不法行为筑起了高墙。

1.2 暗网的危害

维基百科中的资料显示,在所有的暗网网站中,除去占比47.7%的无用数据,非法内容的占比极高,其中与毒品相关的内容占比高达8.1%,与极端主义相关的内容占2.7%,与非法色情相关的内容占2.3%,与黑客相关的内容占1.8%,与武器相关的内容占0.8%,与暴力相关的内容占

0.3%,与其他非法咨询相关的内容占3.8%。暗网中存在的非法活动远远超出了我们的想象,其非法活动的内容更是令人发指。

1.2.1 暗网已成为各色刑事犯罪活动的温床^[5]

2006年,“农夫市场”诞生,标志着暗网中的非法活动正在朝着成熟化、商业化的方向发展,一大批暗网网站应运而生。2013年,有“暗黑淘宝”之称的“丝绸之路”被捣毁,其所经营的主要业务如毒品交易、军火贩卖,甚至是器官交易、人口交易等也开始被公众所了解。2017年7月,美国司法部宣布关闭全球最大的暗网交易市场“阿尔法湾”^[6]。截至网站关闭前,该平台中的卖家数量已高达4万人,买家数甚至超过20万人。据保守估计,自2014年该网站投入运营以来,其交易额可达10亿美元。此外,有媒体报道称曾轰动一时的章莹颖绑架案,很可能也与暗网中的人口交易相关。该案件的犯罪嫌疑人是在作案前浏览过网站“绑架101”中相关的帖子,而该网站是捆绑、恋物癖以及另类性癖爱好者的聚集地。

1.2.2 暗网已成为恐怖主义活动的新平台

2015年11月13日晚,法国巴黎的枪击爆炸事件发生后,有证据显示为了规避政府的大规模审查,策划这起事件的伊斯兰国恐怖分子迅速将其宣传机器——生活媒体中心转移到了暗网,并在Shamikh论坛上发布了新的暗网网址及访问方法^[7-8]。该网站后被证明是目前已知的第1个由恐怖组织使用的网站,这说明恐怖主义的犯罪触手已经触及到了暗网世界。更令人感到震惊的是,曾经规模最大的暗网交易市场“阿尔法湾”,不仅是重大的毒品交易聚集地,还是恐怖分子招兵买马、组织和策划恐怖袭击的秘密渠道,其活跃用户中不乏IS等全球闻名的恐怖组织^[9]。除此之外,恐怖分子还常采用备份表层网资源的手段,在暗网上形成镜像,当其在表层网中的宣传网站被关闭后,可以通过电子邮件、匿名论坛等方式发布其在暗网上的镜像网站,为其拥护者和追随者提供新的平台。

1.2.3 暗网已成为大国博弈、政治渗透颠覆的支撑工具

暗网中的意识形态是混乱不堪的,其建立者大都是无政府主义和自由主义的拥护者,这就导致大量意识形态混乱的暗网用户趋之若鹜。其中

也不乏“民主国家”及极端组织别有用心,利用暗网对其他国家进行攻击甚至是对现有政权进行颠覆。例如攻击中国和朝鲜等国家领导人的文章、言论在暗网中层出不穷。被誉为阿拉伯世界革命浪潮的“阿拉伯之春”运动,不仅导致多国政府垮台,也造成100多万人死亡,1500多万人沦为难民。一度成为“公民运动”必备软件的FireChat,可以在密集区域快速自行匿名组网,实现大面积的加密通信。在香港“占中”运动^[10]和台湾“太阳花学运”中起到了重要的作用。在这些运动的背后,都晃动着“民主国家”及组织的身影。暗网及相关技术的出现,为国与国之间的博弈提供了有力的支撑工具。

由此可见,暗网不法行为造成的恶劣影响并不仅仅局限于某个国家地区,还对全球的安全环境构成了巨大威胁。暗网已然成为威胁全球安全的毒瘤。

2 世界各国的暗网治理之策

暗网深不可测,其中隐藏的信息量之多、危害之大远远超出我们的想象。为了治理暗网乱象,很多国家都投入了不小的成本,方法手段也各不相同。但由于暗网与生俱来的特性,导致暗网治理效果不尽如人意。美国国家安全局1份被泄露的文件甚至写道“永远不可能完全揭开所有暗网用户的真实身份”。

2.1 暗网的特性及其治理难题

2.1.1 使用门槛低,受众广且具有隐蔽性

只需简单地安装一个洋葱路由(Tor)软件,暗网世界的大门就被打开了。不需要很高的技术要求,大多数人都可以轻松地进入暗网并使用它,使用暗网的门槛很低。从穷凶极恶的恐怖分子,到贩卖毒品的黑帮头目,再到精神空虚的上班族,甚至是充满好奇心的学生,跨越年龄,跨越国家,越来越多的人带着不同的目的进入暗网世界。用户数量众多,使用目的各不相同,暗网对用户身份匿名性的保护,导致暗网用户身份几乎无法被确定,这无疑对打击网络犯罪增加了不小的难度。

2.1.2 全球化程度高,监管工作无从下手

正如表层网一样,暗网几已渗透到世界的各个角落,几乎涵盖各种形式的犯罪活动,让全球大多数国家陷入其阴影之中。据美国海军研究实验

室和乔治城大学的相关研究人员估计,截至 2013 年 9 月,全球范围内的 Tor 节点数量约有 3 000 个,主要分布在德国、美国和法国,在中国、荷兰、澳大利亚等国也有分布。Tor 全球的用户量约为 95 万,较集中分布在德、中和美国。此外,在日本、意大利和英国等国家也有较广泛的分布。网络无国界,暗网犯罪同样也涉及到了全球范围,其监管工作并非是单一国家能够完成的。

2.1.3 隐藏信息庞大,犯罪成本低,利益巨大

如果说互联网是一座巨大的冰山,表层网只是露出水面的冰山一角,深网才是隐藏在水面之下的真正主角。虽然暗网只占到深网的一小部分,但是由于它暗藏在深网之中,其中包含的海量的、隐蔽的、不可预知的信息,吸引着各种各样的,尤其是怀有不法企图的用户在其中从事隐秘的网上活动,以规避互联网的审查。暗网的无界性给犯罪分子实施跨国犯罪提供了便利条件,大规模犯罪活动带来的丰厚收益又会催生更多、性质更加恶劣的犯罪活动。如此循环,暗网犯罪规模会越来越大,治理难度也会越来越高,仅凭单一国家的力量几乎不可能对其进行有效打击。

2.1.4 网络结构独特复杂,难以被定向摧毁

不同于一般的互联网,暗网的网络结构是分散式的,且其中一切数据的传输都是匿名且无迹可寻的。这意味着,暗网的安全性较普通互联网更强,想要对其实施定向攻击几乎是不可能的。最常用于暗网访问的 Tor 软件,可以对网络中的流量实现三重加密,且能够通过全球范围内的终端进行传播。因此,想要追踪到某一流量的来源几乎是不可能的^[11]。2013 年棱镜门事件中流出的文件表明,作为全球互联网实力最强,也是 Tor 技术研发者的美国,也并未发现有效途径对其进行破解^[12]。当前看来,并无有效的方法根治暗网。暗网独特的网络结构以及匿名性为网络犯罪提供了得天独厚的条件,想要借助传统的技术方法和执法手段完全摧毁暗网任重道远。新型的暗网犯罪活动还在不断地产生。

除此之外,随着暗网及其相关技术逐渐成为意识形态渗透和大国博弈的新途径,不少国家对暗网犯罪活动视而不见,甚至主动引导其朝着有利于本国利益的方向发展,这直接关闭了打击暗网犯罪活动的入口。

2.2 美俄英法等网络大国的暗网治理手段

尽管暗网治理困难重重,很多国家仍然在探索有效的治理方案。为了打击暗网犯罪活动,美国政府投入了大量的人力物力,加强对暗网通信的监听,致力于达到对每一个节点的监控。2013 年 8 月,美国国家安全局承认其对 Tor 网络进行了监听。之后在 2015 年初,美国发布了一个专门用于搜索暗网内容的搜索引擎“Memex”^[13],该引擎由国防部先进研究项目局(DARPA)开发,试图通过挖掘普通搜索引擎检索不到的内容,打开暗网治理的大门。高强度的监听确实可以有效打击暗网非法活动,但也有很多人认为这是对公民隐私权的侵害,反对的呼声很高。保护公民隐私权和网络空间安全之间的矛盾,导致美国政府在针对暗网治理的问题上也并无上策。

与美国相比,俄罗斯的做法更为强硬。其于 2014 年 2 月通过的一项法案规定,在特殊时期,政府有权切断境内全部互联网;日均访问量超过 3 000 人次的网站所有者,必须实名向政府备案。巴黎恐怖袭击发生后,法国也加紧了暗网治理的脚步。2015 年 2 月通过的反恐新法中明确规定,法国国会可以在紧急情况下正式授权其政府关闭所有与恐怖主义相关的网络通信服务,以应对那些隐藏在暗网中的加密信息传输。英、德等国也意识到了暗网带来的巨大危害,纷纷采取行动,增拨用于打击网络犯罪和网络恐怖主义的资金,扩充网络情报领域规模,建设功能更为健全的网络中心。2017 年,英国国家犯罪局(NCA)为打击暗网中的毒品交易和其他不法行为,招募了大批暗网分析师和网络专家。与此同时,NCA 还成立了专门的暗网情报部门,旨在通过与其他情报和执法部门联动,有效打击暗网犯罪^[14]。除此之外,一些国家也试图通过国际执法合作应对暗网犯罪。2016 年 11 月 1 日,美国联邦调查局官网发布消息称,他们加入了一场由五眼联盟(FELEG)发起的打击暗网非法活动的运动。该联盟成员包括美、英、澳、加拿大以及新西兰的国际执法机构,联盟旨在通过跨国情报共享的方式打击国际犯罪。

2.3 中国的暗网治理手段

表面看来,暗网对我国的影响较之西方国家并不太大,但互联网的无界性每时每刻都在突破中国构建的网络安全现状。关于如何进入暗网的

“教程”越来越多地出现在各公开论坛以及群聊中,涉及到暗网内容的语言和图片宣传更是层出不穷,突破我国互联网管控使用暗网的网民数不断上升;2016年,中国警方查获了一起利用暗网传播儿童色情影像的案件,犯罪嫌疑人之一的孙某竟是北京某大学的学生;此外,中国也是暗网犯罪的受害者,每年都有许多中国公民通过暗网人口黑市被交易,也有许多公司和个人成为经暗网交易的勒索软件的勒索目标;暗网所构成的威胁不受地域限制,作为网络空间中的重要一员,中国不可能独善其身。

2017年6月1日,我国颁布实施的《中华人民共和国网络安全法》^[15]规定,所有用户都需实名上网,从法律层面确定了使用暗网在我国的不合法性。暗网的去中心化和匿名性以及网站建立的随意性都与我国互联网建设、使用、运营、维护的基本要求相悖。事实上,中国从没有放松对暗网犯罪的打击,而是积极投身于治理暗网不法行为的国际合作中。

3 构建“网络空间命运共同体”,搭建暗网治理的有效平台

暗网交易的恶劣性,使其治理迫在眉睫。但暗网的匿名性,其用户群体的多样性,其犯罪活动的大规模、无国界性,又导致其治理不是一蹴而就,也不是单一国家能够完成的。对于如何治理暗网乱象,不同国家都有其各自的思路和方法。中国作为一个负责任的大国,在国际上一直扮演着积极的角色,“和平”“共赢”一直是中国坚持的重要原则。构建“网络空间命运共同体”理念的提出,无疑为暗网治理提出了中国思路。

3.1 构建“网络空间命运共同体”是全球化发展的历史必然

在党的十八大报告中,习近平总书记代表党中央首次提出“人类命运共同体”的思想^[16-17],并指出:“合作共赢,就是要倡导人类命运共同体意识,在追求本国利益时兼顾他国合理关切,在谋求本国发展中促进各国共同发展,建立更加平等均衡的新型全球发展伙伴关系,同舟共济,权责共担,增进人类共同利益^[18]。”2015年12月16日,在以“互联互通、共享共治——构建网络空间命运

共同体”为主题的第二届世界互联网大会上,习近平主席首次提出了“网络空间命运共同体”^[19]的设想,他强调“网络空间是人类共同的活动空间,网络空间前途命运应由世界各国共同掌握。各国应该加强沟通、扩大共识、深化合作,共同构建网络空间命运共同体”,提出了推进全球互联网治理体系变革应该坚持的“四项原则”以及构建网络空间命运共同体时应坚持的“五点主张”^[20]。“网络空间命运共同体”的提出,充分体现了中国对于网络空间重要性的认识,顺应全球化发展的历史潮流。其中促进互联互通、促进共同繁荣、促进公平正义等原则,又体现了中国作为一个负责任大国的形象以及坚持和平崛起的决心。“网络空间命运共同体”的提出无疑为乱象丛生的网络空间,尤其是暗网空间治理提出了新的思路,为维护国家和世界网络安全,维护世界和平提供了中国方案。

3.2 “网络空间命运共同体”下的暗网治理需要共管共享

互联网的全球性发展意味着暗网治理并不是仅靠一国之力能够完成的。如何求同存异,将意识形态各异、发展各异、经济水平各异的各国凝聚起来,共同应对暗网治理难题,是世界各国共同关注的问题。而“网络空间命运共同体”的提出,就是要突破国家的界限,合理对待国家间的利益差异,建立以合作共赢为核心的新型网络空间关系。真正做到各国共同掌握网络空间发展方向,共同书写网络空间规则,共同处理网络空间事务,共同分享网络空间发展成果^[21]。

3.2.1 制定国际间共同机制和行为准则

“没有规矩不成方圆”。问题的解决离不开法律与规章,暗网治理也是如此。对于暗网治理,每个国家的法规、条例和治理力度都各不相同。以暗网特有的匿名性为例,不同国家有着不同的法律规定。在我国,《中华人民共和国网络安全法》明确规定所有用户必须实名上网,“用户不提供真实身份信息的,网络运营者不得为其提供相关服务。”这也就意味着那些匿名用户以及其他作为匿名基础设施的暗网服务等,在我国均是违法的。但是在美国等西方国家,匿名表达权却以宪法判例的形式被确定成为一种公民权利。而某些网络技术十分落后的国家,甚至没有针对该行为的法律或管理制度。因此,各国之间亟须建立一种“网络空间共

治”的逻辑,即制定国际网络治理的统一的行准则,以应对暗网的匿名性、无界性特征。将现实中的主权范围对应到网络空间中,划分各国的网络主权范围。对于各国网络主权范围内的暗网非法行为,按各国规定进行处罚,而对于主权范围外的暗网非法行为,则要根据国际间的共同准则予以打击。如同习近平主席在第二届互联网大会中所谈到的:“国际网络空间治理,应该坚持多边参与,由大家商量着办,发挥政府、国际组织、互联网企业、技术社群、民间机构、公民个人等各个主体作用,不搞单边主义,不搞一方主导或由几方凑在一起说了算。各国应该加强沟通交流,完善网络空间对话协商机制,研究制定全球互联网治理规则,使全球互联网治理体系更加公正合理,更加平衡地反映大多数国家意愿和利益。”

3.2.2 依靠技术创新、技术共享,挤压暗网生存空间

暗网匿名保护技术不断进步。近几年不断升级的 Tor 版本,使暗网接入防屏蔽功能不断得到改善,想要限制用户访问暗网的难度不断提高。犯罪者可以在暗网保护下发布、传播有害信息,而不在其中留下任何罪证。执法机构可以用来对抗如此完善的匿名保护机制的技术手段非常有限,线上侦查的成本十分高昂。针对暗网具有的匿名性特点,一些国家虽然想要通过实名认证的方式,用法律手段限制并控制用户对暗网的使用,但可跨国界互联的网络却仍然可以为用户提供多种技术手段访问暗网服务,并且关于该做法是否侵犯公民匿名表达权的纷争也从未断绝。由此可见,仅靠制度规范,并不能从根本上解决暗网治理难题,提高技术才是关键。例如,各国可以考虑建设一个可信的第三方监管机构,需要匿名的用户可以采用实名身份在第三方处申请服务。其实名信息由加密算法进行保护,除非个人授权或是司法程序必要,否则任何人都无权查看。这样一来,既能够保护公民的匿名表达权,也让犯罪分子无机可乘。但是不论是第三方匿名保护或是直接技术对抗,都需要极高的技术要求。大多数国家,尤其是发展中国家,并没有足够的技术及经济基础做支撑。它们更容易成为暗网犯罪攻击发达国家的突破口。“网络空间命运共同体”的核心理念之一便是共担责任,共享繁荣^[22]。这意味着在暗网治理的过程中,

各国都要参与进来,贡献自己的技术力量,不能搞网络霸权主义和平均分配。技术发达的国家要主动承担更多的责任,帮助发展落后国家的技术;落后国家也要积极承担力所能及的工作,维护本国的网络空间利益,不能毫无作为,听之任之。

3.2.3 加强国际间交流,提高防御和态势感知能力

《汉书·项籍传》有云:“先发制人,后发制于人。”该思想也同样适用于暗网治理,如果能够建立一个暗网犯罪全球态势感知体系,就意味着监管者可以根据之前获得的暗网犯罪情报,预测出可能会出现暗网犯罪的目的和手段变化。这样一来,决策者便可以及时调整针对暗网犯罪的策略,暗网治理体系的防御能力将会大大提高。从而真正达到构建“网络空间命运共同体”的核心目标——合作共赢^[23]。但是要想构建完整的态势感知体系,需要综合全球各国的情报信息。可能有些情报的获取成本比较高昂,有些情报的获取难度较大,导致部分国家不愿与其他国家进行情报共享。对于此种情况,网络大国应积极做信息共享的示范者、引领者,主动承担情报共享及其他相关工作,呼吁各国参与到暗网治理体系的构建中去,以有效应对日益猖獗的暗网犯罪。

网络的连通性和全球性决定了网络安全问题的影响也是全球性的。全球问题只能全球治理。在处理网络安全问题时,任何国家都不能“只扫门前雪”,尤其是打击暗网不法行为,更需要各国联合起来。习近平提出的构建“网络安全命运共同体”思想,目的就是要在平等互信、相互尊重主权安全的基础上,构建国家之间共同的网络安全规则和标准,加强国际间技术和信息的交流与合作,共同打造国际网络安全平台,为维护世界和平与安全提供中国思路,彰显中国力量。

参 考 文 献

- [1] 陶春. “互联网女皇”的报告,带你认识互联网趋势[J]. 中国教育网络, 2017 (7): 5-7
- [2] Bergman M. The deep Web: Surfacing hidden value [J]. The Journal of Electronic Publishing, 2001, 7(1): 1-17
- [3] 秉泽. “暗网”: 你所不了解的互联网[J]. 保密工作, 2016 (2): 47-48
- [4] 陈海强. 暗网: 生存还是死亡? [J]. 中国信息安全, 2017 (11): 61-64

- [5] 黄伟. 暗网世界的黑色犯罪[J]. 检察风云, 2017 (23): 14-17
- [6] 陶凤. 暗网黑市全球“剿匪记”[N]. 北京商报, 2017-07-24 (8)
- [7] Ragan S. After Paris, ISIS moves propaganda machine to Darknet [EB/OL]. [2018-03-20]. http://www.csoonline.com/article/3004648/security-awareness/after-paris-isis-moves-propaganda-machine-to-darknet.html#tk.rss_all
- [8] 肖洋. “伊斯兰国”的暗网攻势及其应对路径[J]. 江南社会学院学报, 2017, 19(1): 19-23, 37
- [9] 杨亚强. 暗网恐怖主义应对路径探析[J]. 江西警察学院学报, 2017 (4): 55-60
- [10] 焦康武. 总体国家安全观视域下我国暗网犯罪应对研究[J]. 犯罪研究, 2017 (6): 78-89
- [11] 暗网的养成. Tor(洋葱路由)的故事[J]. 中国信息安全, 2017 (11): 65-68
- [12] 王丹娜. 暗网治理需各国执法协同联动[J]. 中国信息安全, 2017 (11): 77-80
- [13] Paganini P. Memex—The new search tool to dig also in the Deep Web [EB/OL]. [2018-03-10]. <http://securityaffairs.co/wordpress/33336/cyber-crime/darpa-memex-deep-web.html>
- [14] 周兆军. 英国向三大情报机构额外拨款应对恐怖袭击威胁 [EB/OL]. [2018-03-16]. <http://www.chinanews.com/gj/2015/11-16/7626267.shtml>
- [15] 中华人民共和国网络安全法[N]. 人民公安报, 2016-11-08 (3)
- [16] 张展. 新时期“人类命运共同体”的内涵及意义探析[J]. 决策探索, 2017 (6): 21-23
- [17] 王义桅. 人类命运共同体的内涵与使命[J]. 人民论坛·学术前沿, 2017 (12): 6-12
- [18] 高惠珠, 赵建芬. “人类命运共同体”: 马克思“共同体”思想的当代拓新[J]. 上海师范大学学报: 哲学社会科学版, 2017, 46(6): 18-23
- [19] 徐隽. 习近平出席第二届世界互联网大会开幕式并发表主旨演讲[N]. 人民日报, 2015-12-17(1)
- [20] 董慧, 李家丽. 新时代网络治理的路径选择: 网络空间命运共同体[J]. 学习与实践, 2017 (12): 37-44
- [21] 惠志斌. 全球治理变革背景下网络空间命运共同体构建[J]. 探索与争鸣, 2017 (8): 98-102
- [22] 本刊综合报道. 激荡时代梦想 照亮未来生活 第四届世界互联网大会携手共建网络空间命运共同体[J]. 中国科技产业, 2017 (12): 12-13
- [23] 王照明. 习近平网络空间命运共同体思想的交往理性及其文明逻辑[J]. 哈尔滨市委党校学报, 2017 (4): 13-18



周琳娜

教授, 主要研究方向为网络空间安全、信息隐藏、数字取证。
zhoulinna@tsinghua.edu.cn



高存

硕士研究生, 主要研究方向为网络空间安全、数字取证。
gaocun_uir@163.com