·专题研究·

非洲网络安全治理初探*

肖莹莹　袁正清

内容提要　非洲互联网发展起步晚、普及快，与之相伴随的是网络犯罪日益猖獗、相关法律制度及执法能力滞后、公众和企业网络安全意识相对薄弱的现状。近年来，非洲各行为体开始加快设计网络安全治理方面的制度框架。除了电子交易和网络犯罪外，个人数据保护也是非洲网络安全治理的重要内容，这和西方发达国家的“传授”以及非政府组织的积极倡导有关。非洲网络安全治理的制度设计中，不论是在国家层面、次区域组织层面、非盟层面，还是非政府组织层面，都有西方发达国家和西方主宰的国际组织的身影，部分制度的内容借鉴甚至照搬了西方国家原有的设计。这可能造成非洲大陆在网络空间被再度“殖民化”。而且，根据西方经验设计的制度是否适合非洲国家的文化和观念，还有待于实践的检验。

关 键 词　网络安全　网络犯罪　数据和隐私保护　治理路径　非洲联盟

作者简介　肖莹莹，中国社会科学院研究生院博士生（北京　102488）；袁正清，中国社会科学院世界经济与政治研究所研究员（北京　100732）。

随着信息通讯技术的迅猛发展，网络已经成为世界各国经济社会发展的重要基础。在网络空间中，由于网络攻击者的匿名性、网络归因溯源技术的

*本文系袁正清主持的国家社科基金项目“国际组织分析的社会学路径研究”（11BGJ003）的阶段性成果。

受限性以及网络空间本身的互联互通性，网络安全[①]具有全球性和无国界性的特点。这意味着，任何一个国家或地区的网络安全治理状况都与其他地方休戚相关，非洲大陆也不例外。近年来，随着非洲大陆互联网普及率的大幅提高，以及国际社会对网络安全治理的日益重视，非洲各行为体也开始加快设计网络安全方面的制度框架，了解和掌握这些最新进展对于中国而言具有很强的现实意义。

从国内外的研究情况来看，2010 年以前，研究非洲网络问题的学术文章基本上都在讨论信息通讯技术对非洲经济发展、教育、医疗等方面的影响，或者非洲大陆在弥合“数字鸿沟”方面面临的机遇与挑战等，关注非洲网络安全的学术类文章很少，从治理的角度谈论非洲网络安全的文章更是屈指可数。2010 年之后，国外学术界开始较多地出现与非洲网络安全（特别是网络犯罪）有关的文章。这些文章的特点是：多为国别研究、描述性介绍，且是对具体事件的短评或者一些研讨会的简短报告，在系统性和理论性方面均存在有待完善之处。国内学界对非洲网络安全的研究更为落后，在中国知网（CNKI）上以“非洲”、“网络”和“安全”为关键词进行搜索，相关文章非常少。

非洲大陆的网络安全现状如何？为了开展网络安全治理，非洲在不同层面做出了怎样的制度安排？还面临怎样的问题和挑战？这些都是本文所要研究的问题。

非洲网络安全治理的现状与理念

（一）非洲网络安全现状

每个国家和地区的网络安全状况都与其互联网发展水平有着密切关系，非洲国家亦是如此。由于经济基础薄弱，非洲信息通信业的发展一直以来都落后于世界其他地区。近年来，由于非洲地区铺设了多条联通其他大陆的海底光缆以及连接内陆国家的陆地光缆，宽带网络的覆盖率大幅提升，非洲地区的互联网用户数量迅速增加。截至 2014 年 12 月 31 日，非洲互联网用户超

① 本文从广义的角度理解网络安全，即网络安全包括网络犯罪、网络间谍、网络恐怖主义、网络战争、在线隐私和数据保护等若干形式。

过3亿，较2000年底的数据增长6 958.2%，增速居全球首位，但互联网普及率（互联网用户占当地人口的比率）仅为27.5%，仍为全球最低水平。[①] 除了互联网普及率总体落后之外，非洲各国间的互联网发展水平也存在较大差异。截至2014年6月底，非洲互联网普及率较高的国家包括马达加斯加（74.7%）、马里（72.1%）、马拉维（70.5%）、摩洛哥（61.3%）、塞舌尔（54.8%）、埃及（53.2%）和南非（51.5%），均高于同期中国的互联网普及率（47.4%）。但非洲也是互联网普及率低于2%的国家数量最多的大洲，包括埃塞俄比亚（1.9%）、几内亚（1.8%）、尼日尔（1.7%）、塞拉利昂（1.7%）、索马里（1.6%）等国。[②] 非洲互联网发展的另一特点是，移动终端为主要的上网途径。非洲绝大多数地方都没有经过固网的发展阶段而直接进入移动互联网时代，多数非洲人首次“触网”都是通过他们的手机。这与非洲大陆独特的地理环境、陆地光缆不发达、电力供应不够稳定、手机比电脑价格低等多种因素有关。目前，非洲是全球移动互联网增速最快的区域。国际电信联盟的数据显示，从2011年到2014年，非洲的移动互联网订户增长超过40%，是全球平均水平的两倍；2014年，非洲的固网普及率只有0.4%，而同期非洲的移动互联网普及率已从2010年的2%增至近20%。[③]

正是由于非洲互联网建设起步晚、发展快，该地区才会存在网络犯罪异常猖獗、相关法律制度及执法能力滞后、公众和企业网络安全意识相对薄弱等诸多问题。具体而言，非洲地区的网络安全具有以下几个特点：

第一，网络犯罪[④]是非洲网络安全治理的重点。就网络犯罪的具体形式而言，近年非洲的网络犯罪大多和金融诈骗相关，数字化程度相对较低。从技术层面来看，比较严重的网络犯罪对带宽设备和互联网普及率有一定要求，

① Http://www.internetworldstats.com/stats.htm, 2015-06-19.

② Ibid.

③ ITU, “The World in 2014 ICT Facts and Figures”, http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf, 2015-04-17.

④ 网络犯罪的概念有狭义和广义之分。狭义的概念是指侵犯网络数据和系统的机密性、完整性以及可使用性的犯罪行为，比如黑客开展的各种网络攻击行为；广义的概念是指借助网络数据和系统开展的任何犯罪行为，除了狭义概念涉及的内容外，还包括那些通过使用网络使传统犯罪具备新属性和冲击力的犯罪行为，比如借助网络开展的金融欺诈、毒品走私、人口贩卖等犯罪行为。本文采用的是广义的网络犯罪概念。

10% ~15% 的互联网普及率是大规模黑客活动的最低要求。[①]由于多数非洲国家没有铺设光纤电缆，只能依赖速度较慢的卫星连接方式，这意味着攻击当地网站时需要的时间更长。从网络犯罪分子的角度来说，这种条件对于有效开展网络攻击是很不可靠的，因此“419 诈骗”[②] 是前些年非洲网络犯罪的主要形式之一，这种犯罪形式只是将电子邮件作为诈骗的传播途径，还需要罪犯和受害者之间的互动。但是，近年来，随着数条光纤海底电缆和陆地电缆的铺设完成，非洲越来越多的有组织犯罪集团（包括海盗、恐怖分子、毒品走私贩以及人口贩卖团体等）开始借助互联网开展犯罪活动。由于这些犯罪分子掌握了更加高级的手段（如恶意代码和僵尸邮件），网络犯罪的形式日渐升级，频率也迅速提升。卡巴斯基实验室的数据表明，2014 年第一季度非洲大陆发生了超过 4 900 万次网络攻击，其中大部分发生在阿尔及利亚，其次是埃及、南非和肯尼亚；网络犯罪在南非最为猖獗，网络安全公司诺顿称，70% 的南非人都曾是网络犯罪的受害者，而全球的平均数是 50%。[③] 特别是随着移动互联网用户的增加，手机银行正成为网络犯罪分子的新目标。非洲很多金融机构的应用程序都没有做好安全工作，缺乏加密程序，容易遭受恶意“钓鱼”攻击。

第二，非洲公众和企业的网络安全意识较弱，国家和地区层面缺乏合适的法律框架，并且存在能力建设不足的问题。尽管非洲拥有众多网吧，但供应商多数时候未能提供适当的杀毒软件，致使这些电脑很容易成为僵尸网络操控者及黑客的目标。据网络安全专家估计，非洲大陆约 80% 的个人计算机都已遭病毒入侵或者被植入恶意程序。[④] 一旦这些计算机被有不良意图的个人或组织劫持，这些僵尸电脑便会被人任意控制，用来发送垃圾邮件或病毒。此外，非洲国家和地区层面还缺乏完善、协调一致的法律框架，执法机构的

---

① M Reilly, “Beware, Botnets Have Your PC in Their Sights”, *New Scientist*, Vol. 196, 2007, pp. 22 - 23.

② “419 诈骗”也称“尼日利亚诈骗”，源于尼日利亚颁布的专门禁止金融诈骗的第 419 号法律。这是一种从 20 世纪 80 年代就开始流行的金融诈骗手段，因源于尼日利亚而得名，与该国并无直接关系。诈骗者通常会声称有一笔巨款需要转账，向诈骗对象承诺只要事先支付一笔费用，就可以获得数量可观的佣金。在取得信任后，诈骗者就会以各种理由收取手续费或其他费用，待行骗成功后，骗子立即消失得无影无踪。

③ Tom Jackson, “Can Africa Fight Cybercrime and Preserve Human Rights?”, April 10, 2015, http: //cybersecuritycaucus. com/can - africa - fight - cybercrime - and - preserve - human - rights, 2015 - 06 - 02.

④ 斯蒂芬·加迪：《世界最大僵尸网络或藏非洲》，柴志廷译，载《世界报》2010 年 4 月 14 日。

人员、情报和基础设施都配置不足。[①] 联合国毒品和犯罪问题办事处（UNODC）开展的一项调查显示，半数以上的非洲国家认为自己调查网络犯罪的执法资源不足，所有的非洲国家表示需要技术援助，特别是调查网络犯罪方面的技术。[②]

第三，在西方发达国家的“传授”和以当地非政府组织为代表的公民社会倡导下，隐私和数据保护等成为非洲网络安全的重要内容。与原来的草案相比，非盟2014年6月通过的《关于网络空间安全和个人数据保护的公约》中加入了数据保护的内容，从而使非洲成为欧洲之外第一个通过数据保护公约的地区。目前，14个非洲国家已经拥有隐私框架法律和某种类型的数据保护主管机构，一旦非盟公约经成员国批准生效后，很多其他国家很可能也会根据公约的要求制定数据保护法。分析人士认为，非盟公约复制的是欧盟的数据保护模式，即每个成员国都拥有本国的数据保护法和管理机构。[③]

第四，与隐私和数据保护多受西方影响不同，电子交易和打击网络犯罪等内容是非洲各利益攸关方出于自身现实需要建构的网络安全内容。日益猖獗的网络犯罪问题已经让非洲国家认识到，必须建立相关的法律法规确保电子交易和网络环境的安全，才能推动互联网经济的快速发展并从中获益。同时，与西方国家以及上合组织成员国相比，非洲国家对网络战争、网络恐怖主义等问题的关注程度较低，这实际上是非洲国家在安全治理中普遍重视低级政治问题、无暇顾及高级政治问题的体现。

（二）非洲网络安全的理念

2014年6月，在赤道几内亚首都马拉博召开的非盟峰会上通过了《非盟关于网络空间安全和个人数据保护的公约》[④]，虽然公约中含有网络安全的字

---

① Fawzia Cassim, “Addressing the Growing Spectre of Cyber Crime in Africa: Evaluating Measures Adopted by South Africa and Other Regional Role Players”, *The Comparative and International Law Journal of Southern Africa*, Vol. 44, No. 1, March 2011, p. 127.

② UNODC, “Comprehensive Study on Cybercrime (draft)”, February 2013, p. xxiii, http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf, 2015-06-17.

③ Cynthia O'Donoghue, “New Data Protection Laws in Africa”, 19 February, 2015, http://www.technologylawdispatch.com/2015/02/regulatory/new-data-protection-laws-in-africa, 2015-06-02.

④ African Union, “African Union Convention on Cyber Security and Personal Data Protection”, pp. 1-3, http://pages.au.int/sites/default/files/en_AU%20Convention%20on%20CyberSecurity%20Pers%20Data%20Protec%20AUCyC%20adopted%20Malabo.pdf, 2015-06-19.

眼，但是全文并没有对“网络安全”的概念做出解释，我们只能从公约文本的相关内容中推测非盟国家对网络安全的理解与看法。公约前言中提到，“认识到公约旨在监管一个快速发展的科技领域，目标是满足有着不同利益的众多行为体的高水平期待，公约阐述了在电子交易、个人数据保护和打击网络犯罪方面建立可信数据空间必不可少的安全规则”。这在某种程度上说明，非盟建构的网络安全概念主要包括电子交易、个人数据保护和网络犯罪这三大领域。

非洲的次区域经济组织在该地区的集体安全机制中亦扮演着重要角色。这些次区域经济组织建构的网络安全强调的也是电子商务、网络犯罪、数据保护等方面。例如，2009 年，东非共同体在非洲次区域经济组织中第一个通过了网络法框架。该框架提出，非洲的网络安全理念分为两个阶段，第一阶段涵盖电子交易、电子签名和鉴定、网络犯罪、数据保护和隐私；第二阶段涵盖知识产权、竞争、电子税务和信息安全。[①] 南部非洲发展共同体 2012 年在博茨瓦纳召开的部长会议上通过了关于数据保护的示范法、关于网络犯罪的示范法和关于电子交易的示范法。西非国家经济共同体也已经设立关于电子交易的法律框架（Supplementary Act A/SA. 2/01/10）、关于网络犯罪的法律框架（Directive 1/08/11）和关于个人数据保护的法律框架（Supplementary Act A/SA. 1/01/10）。[②]

部分非洲国家制定的网络安全政策或法规中虽然包含对网络安全的定义，但用语模糊，解释空间较大，可以被视为包括电子商务、网络犯罪、数据保护甚至更多内容。比如，南非电信部 2009 年推出的网络安全政策指出，“网络安全”指的是保护数据和系统免于未经授权的准入、使用、公开、破坏、修改，或者免于遭受互联网被破坏的影响。[③] 肯尼亚信息通讯技术部 2014 年提出的《国家网络安全战略》将网络安全定义为：保护以计算机为基础的设

① UNCTAD, “Harmonizing Cyberlaws and Regulations: the Experience of the East African Community”, 16 August, 2013, p. iii, http://unctad.org/en/pages/PublicationWebflyer.aspx? publicationid = 251, 2015 - 06 - 19.

② ECOWAS, “Strategy on Cybersecurity”, July 21, 2014, http://www.africatelecomit.com/ecowas - strategy - on - cybersecurity, 2015 - 04 - 20.

③ The Department of Communications of the Republic of South Africa, “Cybersecurity Policy of South Africa”, August 2009, p. 18, http://www.ellipsis.co.za/wp - content/uploads/2011/02/CYBER - SECURITY - POLICY - draft.pdf, 2015 - 06 - 02.

备、信息和服务免受意想不到的或未经授权的准入、改变或破坏的过程和机制。①

非洲学者也曾对网络安全概念做出过界定。尼日利亚学者奥拉米（Olayemi）提出，网络安全是指保护网络空间，使其免受威胁，通常包括三方面内容：旨在保护计算机、计算机网络、相关软硬件设备和其中包含的信息、软件和数据，使其免受各种威胁（包括对国家安全的威胁）的一系列活动和措施；开展这些活动和应用这些措施给上述对象带来的保护程度；在相关领域开展的包括研究和分析在内的各种专业活动。② 他还指出，网络安全的内涵不只是信息安全或数据安全，但和后两者也存在密切关系，因为信息安全是网络安全的核心。由此可见这位非洲学者阐释的是广义的网络安全概念：网络安全是要保护计算机等免受各种威胁（包括对国家安全的威胁），意味着网络战争、网络犯罪、网络间谍等活动都应当在其范畴之内。

非洲网络安全的治理路径

由于非洲多数国家的脆弱性、安全治理自主权向非洲的回归与安全外部依赖性的并存，非洲形成了一种包括全球体系、非洲大陆、非洲次区域、非洲国家、非政府组织等公民社会、私人行为体等6个层次的多层安全治理体系。其中，私人行为体指的是参与非洲传统安全问题的私营军事公司，它们介入非洲各类武装冲突，发挥着独特的作用。③

网络安全是非传统安全的一部分。若依照上述层次分析法，非洲网络安全治理形成的是除私人行为体之外的5层安全治理体系，但非洲大陆、次区域、国家和非政府组织4个层次的治理体系中都存在同全球体系（联合国、欧盟等）的合作，因此本文将全球体系视为影响前面4个层次网络安全治理的外部因素，主要从国家、次区域组织、非盟以及非政府组织4个层次分别论述非洲网络安全治理的路径（制度设计）。

---

① Kenyan Ministry of Information, Communications and Technology, "National Cybersecurity Strategy", 2014, p. 17, http://www.icta.go.ke/wp-content/uploads/2014/03/GOK-national-cybersecurity-strategy.pdf, 2015-06-02.

② John Olayemi Odumesi, "A Socio-technological Analysis of Cybercrime and Cyber Security in Nigeria", *International Journal of Sociology and Anthropology*, Vol. 6, No. 3, March 2014, pp. 118-125.

③ 王学军：《非洲多层安全治理论析》，载《国际论坛》2011年第1期，第9~12页。

在现实生活中，上述不同层面的制度设计并不是绝对独立的，它们之间也存在相互借鉴、影响的关系。比如，各国国内立法会以次区域组织和区域组织的制度框架为依据，非盟公约也在制定的过程中以次区域组织已有的制度框架为参考，等等。此外，各类治理主体还在地区性和全球性的多边论坛上加强互动，比如非洲互联网治理论坛（AfIGF），等等。

（一）国家层面

由于多数非洲国家都在忙于应对贫困、艾滋病、能源危机、政治不稳定、民族冲突以及传统犯罪等更为紧迫的问题，打击网络犯罪的努力有些力不从心，非洲正成为网络犯罪分子的“避风港”。具体而言，非盟虽然缔造了《非盟关于网络空间安全和个人数据保护的公约》，但目前还没有一个非洲国家批准该公约。[①] 非洲大陆的 50 多个主权国家中，仅有 10 个国家——埃及、加纳、肯尼亚、毛里求斯、毛里塔尼亚、摩洛哥、尼日利亚、南非、乌干达和津巴布韦制定了国家网络安全战略，[②] 5 个国家——喀麦隆、肯尼亚、毛里求斯、南非和赞比亚制定了网络犯罪专门法[③]，7 个国家——肯尼亚、马达加斯加、马里、尼日尔、尼日利亚、坦桑尼亚和乌干达有数据保护法。[④]

南非在非洲大陆率先引入了应对网络犯罪的立法，目前拥有多个与网络犯罪、数据隐私保护相关的专门法。[⑤] 比如，1996 年，南非通过的《宪法》中就包含保护隐私的内容。2000 年，南非通过了《推进信息准入权法案（修正案）》，以使《宪法》第 32 条有关信息准入的内容生效。2002 年的南非《电子通讯和交易法案》旨在给电子通讯和交易提供便利并开展监管。同在 2002 年，南非还通过了《截取通讯和提供与通讯相关信息的法案》。2012 年，该国又推出《国家网络安全政策框架》，2013 年颁布了《个人信息保护法案》。

---

① Eric Tamarkin, “The AU’s Cybercrime Response”, *ISS Policy Brief 73*, January 2015, http://www.issafrica.org/uploads/PolBrief73_cybercrime.pdf, 2015-05-04.

② NATO CCD-COE, “Cyber Security Strategy Documents”, Updated on 18 March 2015, https://ccdcoe.org/strategies-policies.html, 2015-04-20.

③ See Dana Sanchez, “Without Laws Governing Cyber Crime, Is Africa Safe for Cyber Criminals?”, February 16, 2015, http://afkinsider.com/88623/without-laws-governing-cyber-crime-africa-safe-cyber-criminals, 2015-06-02; also see Judith M. C. Tembo, “Workshop on Tanzania National Transposition of SADC Model Law”, 4th-5th February, 2013, http://afkinsider.com/88623/without-laws-governing-cyber-crime-africa-safe-cyber-criminals, 2015-04-19.

④ Cynthia O’Donoghue, op. cit.

⑤ “Cyberwellness Profile South Africa”, http://www.itu.int/en/Pages/copyright.aspx, 2015-05-09.

不过，非洲第一大经济体——尼日利亚直到2015年5月才拥有专门的网络犯罪法。在此之前，该国2006年通过的《预付费欺诈及其他相关犯罪法》是尼日利亚唯一一部涉及与互联网犯罪相关内容的法律。事实上，因“419诈骗”等网络犯罪导致国家形象严重受损的尼日利亚，2004年就已成立网络犯罪工作组，旨在建立确保计算机系统和网络安全的法律和制度框架，但由于国内各利益攸关方对网络犯罪法案的条款存在争议，提交参议院的法案文本被多次调整，导致法案迟迟未能通过国民议会的批准。据尼日利亚一家较为活跃的公民社会组织“尼日利亚范式倡议”（Paradigm Initiative Nigeria）透露①，该组织一直呼吁通过强有力且公正的网络犯罪法律，“有关的法律必须足以威慑网络犯罪的发生，但也必须足够公平，不能伤害互联网自由，或者让政府用来打击异己分子”。该组织还表示，未来将推动尼日利亚立法机构通过一项保护公民数字权利和自由的法案。值得一提的是，尽管尼日利亚深受恐怖主义之害②，该国对网络恐怖主义问题的重视程度却不够高，在《网络犯罪法案》中虽有涉及网络恐怖主义的条款，但内容很少，只是提到“为了恐怖主义的目的进入计算机或计算机系统，将被处以20年监禁或者罚款2 500万尼日利亚奈拉，或者二者并罚”。

其他的非洲国家，诸如博茨瓦纳、肯尼亚、乌干达和喀麦隆也开始引入网络立法，建立打击网络犯罪的地区性合作机制。③ 此外，毛里求斯是唯一一个签署并批准《布达佩斯网络犯罪公约》④ 的非洲国家，南非在2001年11月就签署了该公约，但目前尚未批准，摩洛哥和塞内加尔正在考虑加入该公约。

非洲各国的立法会直接或间接地受到区域内外多边制度安排的影响。比如，西非国家在立法的过程中就将《英联邦关于计算机和计算机犯罪示范法》、欧洲委员会（Council of Europe）的《布达佩斯网络犯罪公约》和《西

① “Nigeria's President Jonathan Signs the Cybercrime Bill Into Law”, May 16, 2015, http://techloy.com/2015/05/16/nigerias-president-jonathan-signs-the-cybercrime-bill-into-law, 2015-06-10.

② 《尼日利亚全球恐怖主义指数排名高居第四》，载中国驻尼日利亚大使馆经商参处网站：http://www.mofcom.gov.cn/article/i/jyjl/k/201411/20141100806763.shtml, 2015-04-20。

③ Fawzia Cassim, “Addressing the Growing Spectre of Cyber Crime in Africa: Evaluating Measures Adopted by South Africa and Other Regional Role Players”, pp. 123-124.

④ 欧洲委员会2001年11月通过的《布达佩斯网络犯罪公约》是世界上第一部针对网络犯罪行为国际公约。截至2014年10月，全球共有44个国家签署并批准了该公约，包括美国、日本、澳大利亚等国家。

非国家经济共同体关于打击网络犯罪的指令（2011）》作为指导。[①] 国外有学者研究发现，南非的《电子通讯与交易法》的内容十分接近于英联邦范例法、南部非洲发展共同体范例法和《布达佩斯网络犯罪公约》，尤其和布达佩斯公约的条款相似度最高。[②]

（二）次区域层面

非洲不同区域在冷战期间和冷战后陆续建立了多个次区域组织，比如东非共同体、西非国家经济共同体（简称“西共体”）、中非国家经济共同体、南部非洲发展共同体等。冷战时期建立的次区域组织主要针对经济方面的合作，而冷战后，各次区域组织开始将传统安全和非传统安全作为它们合作的领域，并成为非洲集体安全机制的重要组成部分。

作为非传统安全的一部分，网络安全已被非洲多个次区域组织列入议事日程。尽管次区域组织被视为非洲大陆集体安全机制的辅助性力量[③]，但在推动网络安全合作方面，次区域组织表现出了比区域组织（非盟）更活跃、更灵活的特点，形成了次区域内合作的机制网络。值得关注的是，这些次区域组织在开展网络安全合作时，都得到了欧美等西方发达国家和西方主宰的国际组织的资金和技术支持。

比如，西非国家大多借助西共体来推动网络安全领域的合作。首届西非网络犯罪峰会于 2010 年 11 月 30 日～12 月 2 日在尼日利亚的首都阿布贾召开。会议由西共体、联合国毒品和犯罪问题办事处、尼日利亚经济与金融犯罪委员会（EFCC）和微软公司共同举办，主题是“打击网络犯罪：推动创新驱动和可持续的经济发展”。除了非洲国家外，美国、法国、英国、奥地利、土耳其、阿拉伯联合酋长国等域外国家，联合国毒品和犯罪问题办事处、欧洲委员会、国际刑警组织、欧盟等国际组织也派出代表出席了会议。[④] 2012

---

① UNODC, Comprehensive Study on Cybercrime (draft), p. 74.

② Deutsche Telekom Group Consulting, “Republic of South Africa Review Report: E-commerce, Cybercrime and Cybersecurity - Status, Gaps and the Road Ahead”, 26 November, 2013, https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/south-africa---status-gaps-and-road-ahead-cyber, 2015-06-19.

③ 吕淑平：《试析冷战后非洲大陆集体安全机制》，外交学院 2014 届硕士研究生学位论文，第 18 页。论文提出，冷战后，非洲大陆内部逐渐形成了以非洲统一组织（非洲联盟）为主体力量、以非洲次区域组织为辅助性力量、以区域性大国为核心力量的“三位一体”非洲大陆集体安全机制。

④ “West Africa Takes Lead in Fighting 419 Scams”, http://www.unodc.org/nigeria/en/1st-west-africa-cybercrime-summit.html, 2015-04-08.

年9月和2013年1月，美国国务院先后在塞内加尔的达卡和加纳的阿克拉组织召开了西共体法语国家和西共体英语国家参加的西非网络安全和网络犯罪专题讨论会，共同讨论强化国内立法、建立应急反应机制并且确保推进互联网自由和尊重人权的网络安全全面计划。[①] 2014年，西共体和联合国贸发会议联合举行了旨在帮助西共体国家协调网络立法的研讨会。该研讨会有两个主题，一是各国网络相关立法协调一致，二是强化应对网络犯罪。前者获得联合国贸发会议的资助，后者得到了欧洲委员会的资助。

非洲其他地区预防和打击网络犯罪的项目也得到了西方的资助。2013年8月22~24日，在坦桑尼亚首都达累斯萨拉姆召开了东非国家打击网络犯罪的研讨会，该研讨会由欧洲委员会资助，是非洲网络法和预防网络犯罪中心（ACCP）、欧洲委员会和联合国非洲预防犯罪和罪犯待遇研究所（UNAFRI）的合作项目。在研讨会上，欧洲委员会的《布达佩斯网络犯罪公约》被当作参考资料，对一系列的问题（网络犯罪、电子证据的定义，执行立法过程中的实务等）提供指导。

在欧洲委员会的影响下，非洲多个次区域组织都提出了预防和打击网络犯罪的倡议。比如，东非共同体通过了《东非共同体网络法框架草案(2008)》，西共体通过了《西非国家经济共同体关于打击网络犯罪的指令(2011)》，东南非共同市场也制定了《东南非共同市场网络犯罪示范法(2011)》，南部非洲发展共同体制定了《关于电子商务和网络犯罪的示范法(2012)》。[②] 但只有西共体打击网络犯罪的指令具有约束力。此外，那些不具有约束力的法律文件可以给非洲各国的立法提供参考或范例，当很多国家选择将国内法和范例法协调一致时，不具有约束力的法律文件也能产生重要影响。[③]

关于非洲次区域组织提出的这些倡议和《布达佩斯网络犯罪公约》的关系，有关的研讨会曾经指出，《布达佩斯网络犯罪公约》的精神已经体现在了这些倡议中，这增加了非洲国家加入该公约的可能性，也意味着非洲大陆内

---

① US Department of State, Press Release, West African Cybersecurity and Cybercrime Workshop, January 28, 2013, http://www.state.gov/r/pa/prs/ps/2013/01/203379.htm, 2015-04-08.

② ACCP, Workshop Report on Cybercrime Legislation in West Africa, 11 April, 2014, pp. 31-33, http://tftcal.unctad.org/pluginfile.php/12929/mod_resource/content/2/Workshop%20Report%20by%20ACCP%20Ghana%2018%20-%2021%20March%202014.pdf, 2015-04-21.

③ UNODC, "Comprehensive Study on Cybercrime (draft)", p. 64.

部以及非洲和欧洲委员会之间将会有更进一步的合作。[①]《东南非共同市场网络犯罪示范法（2011）》被认为在国际合作方面的条款很详细，满足了《布达佩斯网络犯罪公约》的所有标准，而且该法还包括了有关消费者保护和服务供应商义务的条款。南部非洲发展共同体关于电子商务和网络犯罪的示范法被认为没有达到《布达佩斯网络犯罪公约》的标准，因为它没有关于国际合作、互助和引渡的条款。[②]

（三）非盟层面

实际上，长期以来在非洲安全构建中扮演主体性角色的非盟将这种角色延伸到了网络安全领域。2014 年 6 月，在赤道几内亚的首都马拉博召开的非盟峰会通过了《非盟关于网络空间安全和个人数据保护的公约》。该公约的最初版本是在 2011 年提出的，但几经修改，最终版之前的草案名为《非盟关于网络空间信心和安全的公约》，本应在 2014 年 1 月通过，由于多方反对，非盟在 2014 年 5 月举行了专家会议，对该公约进行了全面审议，并将其更名。这些反对者主要来自私人部门和公民社会团体，他们认为该公约没有体现他们的意愿，在保护隐私和言论自由方面体现得不够。[③] 比如，来自肯尼亚的非政府组织指出，原来的公约草案给政府赋予了过多权力，特别是获取私人信息的权力。有关条款都允许政府为了国家安全和公共利益的目的，可以在不经过所有者允许的情况下获取个人数据和敏感数据。它们还指出，在非洲，国家安全往往被理解为政权安全，该草案会允许政府获取个人数据和打击异己分子。[④]

在经历多方利益博弈后，非盟最终通过了关于网络空间安全和个人数据保护的公约。非盟公约中很多与数据保护有关的内容都是欧盟相关制度的映照。比如，非盟公约也要求成员国建立独立的国家数据保护机构（DPA），该机构必须拥有广泛的权力，包括调查、评价、警示、通知、罚款等。公约要

---

① Patrick Mwaita and Maureen Owor, "Workshop Report on Effective Cybercrime Legislation in Eastern Africa", 22 - 24 August 2013, pp. 2 - 3, http: //www. coe. int/t/dghl/cooperation/economiccrime/Source/Cybercrime/Octopus2013/2571_EastAfrica_WS_Report. pdf, 2015 - 04 - 20.

② ACCP, "Workshop Report on Cybercrime Legislation in West Africa", p. 32.

③ "African Union Adopts Convention on Cyber Security", 14 July 2014, https: //ccdcoe. org/african - union - adopts - convention - cyber - security. html, 2015 - 04 - 22.

④ Joel Macharia, "Africa Needs A Cybersecurity Law But AU's Proposal is Flawed, Advocates Say", January 31, 2014, http: //techpresident. com/news/wegov/24712/africa - union - cybersecurity - law - flawed, 2015 - 04 - 22.

求数据掌握者“不能转移个人数据”到非盟之外的国家，除非接受国“确保提供恰当水平的保护”，“恰当”一词和欧盟数据保护指令第25条使用的术语一致。①

总体而言，公约中仍存在诸多不足。其一，非盟公约涵盖的范围太过宽泛，包括电子商务、数据保护、网络犯罪等，这使其内容显得冗长烦琐，非洲国家应当首先关注的是其有关网络安全和网络犯罪的条款。② 其二，非盟公约“移植”了西方国家法规制度的很多内容，超出了非洲国家现有的执法能力，这给它们批准和执行该公约制造了困难。其三，该公约必须获得15个非盟成员国的批准才能生效，但目前还没有获得一个国家的批准，这使其前景充满变数。并且，考虑到科技发展的日新月异，等到15个成员国批准该公约之时，有关的制度安排恐怕也已滞后。其四，公约对私营部门和政府间的信息分享没有设防，没有声明在打击网络犯罪时，政府获取信息的权力应该受何限制，这在公民社会看来是“很危险的”。③ 很多情况下，公约似乎将国家主权和裁量权置于国际法之上，比如，在有关推进网络安全和打击网络犯罪的第三章中，公约使用了“所有被认为必要、适宜和有效的方法”的表述。如此宽泛的裁量权就会给予国家（特别是不民主国家）滥用这些权力的空间。其五，由于次区域组织和非盟之间没有直接隶属关系，在实际运作过程中，其制度安排之间可能存在矛盾与冲突。

（四）非政府组织层面

20世纪90年代以来，在西方国家的推动下，非洲非政府组织的功能与影响迅速发展，从人道主义救援、社会服务等有限领域扩展到经济、政治与社会发展等诸多领域，在非洲各国政治生活中的地位大大提升。非洲非政府组织还作为公民社会的代表开始分担非洲国家的社会管理、服务，甚至发挥政治职能。④

非洲非政府组织大多与西方国家政府联系密切。一方面，许多在非洲活动的非政府组织本身就是西方非政府组织在非洲的分支机构。另一方面，多

---

① Graham Greenleaf and Marie Georges, “The African Union's Data Privacy Convention: A Major Step toward Global Consistency?”, *Privacy Laws & Business International Report*, 2014, pp. 18 - 21.

② Eric Tamarkin, “The AU's Cybercrime Response”, p. 4.

③ “Africa Must Improve its Cyber - Security”, *AFK Insider*, Feb. 25, 2015, http://umaizi.com/africa - must - improve - its - cyber - security, 2015 - 04 - 08.

④ 王学军：《非洲非政府组织与中非关系》，载《西亚非洲》2009年第8期，第57页。

数本土非政府组织由西方国家政府或非政府组织提供资金。正因为如此，非洲的非政府组织大多是西方理念的“代言人”。反映在制度设计层面，《非盟关于网络空间安全和个人数据保护的公约》与之前的草案相比，增加了个人数据保护、隐私保护的内容，这些实际上都是西方支持下的非政府组织推动的。在非盟公约通过几周后，非洲从事与互联网安全相关活动的 21 个非政府组织，包括非洲很多著名的人权组织，一起推出了《与互联网权利和自由有关的非洲宣言》。该宣言的 12 条“关键原则”中，有两条涉及保护互联网隐私和数据安全内容。该宣言也包括反对监视（Mass Surveillance）的内容。宣言还提出，要实现这些原则，需要和“已经建立的数据保护原则保持一致”，尽管没有明确点明这些原则所指，但分析认为应该指的是非盟公约中的数据保护原则。①

而且，非洲的非政府组织很少对美国借助互联网名称与数字地址分配机构（ICANN）操纵全球互联网域名及根服务器管理权的行为提出抗议。事实上，目前非洲互联网发展面临的主要挑战之一就是缺少域名系统（DNS，Domain Name System）。非洲互联网络信息中心（Africa Internet Network Information Center，AFRINIC）的统计显示，截至 2012 年 10 月，非洲的国别顶级域名（Country Code Top - level Domains，CCTLD）共有 797 952 个，只占全球总数的 1%；非洲的通用顶级域名（Generic Top - level Domain，GTLD）共 122 144 个，占全球的 0.09%；非洲的第四版互联网协议（IPv4）② 地址共 47 522 304 个，仅占全球的 1%。③ 两相对比，这更能反映出非洲非政府组织的利益倾向性。

非洲网络安全治理面临的挑战

非洲已初步建立网络安全治理的基本框架，但面临的挑战仍很艰巨。这是因为非洲大陆互联网发展状况滞后，制度建设起步较晚，各治理主体做出

① Graham Greenleaf and Marie Georges，“The African Union's Data Privacy Convention：A Major Step toward Global Consistency?”，pp. 18 - 21.

② “IPv4”是互联网协议（Internet Protocol，IP）的第四版，也是第一个被广泛使用且是构成现今互联网技术的基石的协议。

③ “ICANN's Africa Strategy Document V1. 1”，October 2012，http：//www. afrinic. net/index. php? option = com_content&view = article&id = 854，2015 - 06 - 23.

的制度安排目前多数还停留在纸面上，没有真正发挥效力。非盟有关公约2014年刚获得通过，目前还没有生效。次区域组织做出的制度安排多数没有法律约束力，只能给成员国国内立法提供指导。在非洲国家中，拥有网络犯罪或者数据保护专门法的国家少之又少，并且这些拥有立法的国家是否愿意根据区域或次区域制度安排调整本国立法，都还是未知数。非洲互联网治理中面临的挑战主要是：

第一，非洲各利益攸关方（特别是政府）参与网络安全治理国际合作的积极性还有待提高。以区域内国际合作来说，非洲互联网治理论坛（AFIGF）目前仅举办了3届，参与国和参与方的数量都有待增加。[①] 第二届非洲互联网治理论坛的参与者只有195人，分别来自29个国家的政府、私人部门、公民社团、地区性组织和国际组织。第三届非洲互联网治理论坛的参与者达到了470人左右，来自41个国家，数量较上届有较大增加，但与非洲54个国家的总数相比仍有一定差距。在全球性的互联网治理论坛上更是很难听到来自非洲的声音。非洲的利益攸关方当前多采取观望态度，背后的原因有很多，除了缺乏足够的网络治理专家、有其他一些更为紧迫的事情需要应对等原因外，还和非洲政府、政客和媒体将全球网络空间治理视为大国间博弈的场域有关，这种观望态度正在严重影响非洲网络安全治理的进度。[②]

第二，非洲各治理主体受西方国家影响较深，对其倡导的理念、核心关切、制度几乎全盘接受，由此可能造成的后果是：非洲大陆在网络空间再度被“殖民化”，在全球网络安全治理问题上没有自主决策权。欧美国家以帮助非洲国家加强能力建设为借口，“传授”本国经验，借助非洲国家非政府组织的力量推动非洲国家的制度建设。例如，在2014年4月举行的“关于互联网治理未来的全球多利益攸关方会议”（NETmundial）巴西圣保罗会议开始前，有一个开放的提交建议程序，允许所有的利益攸关方提交关于互联网治理原则和改革路线图的意见。当时，会议共收到了180多份材料，其中19份来自

① 第一届非洲互联网治理论坛于2012年在埃及召开；第二届和第三届非洲互联网治理论坛分别于2013年和2014年在肯尼亚和尼日利亚召开。

② Ephraim Percy Kenyanito, “Internet Governance: Why Africa Should Take the Lead”, http://www.circleid.com/posts/20140225_internet_governance_why_africa_should_take_the_lead, 2015-06-19.

非洲——1 份来自政府（突尼斯政府）、9 份来自公民社团组织、3 份来自私人部门、1 份来自技术共同体、1 份来自多利益攸关方平台、4 份来自学术界。[①] 从材料的内容来看，14 份材料与表达自由或人权有关，11 份材料与政府角色有关，5 份材料和安全有关，4 份材料和网络中性、可支付的准入、互联网名称与数字地址分配机构的全球化有关，1 份材料和互联网数字分配机构功能的全球化有关。所有这些材料都认为，让所有利益攸关方参与网络治理进程很重要，并且支持治理模式的分散化。由此可见，非洲国家的理念、核心关切和西方国家有很高的相似度。唯一的例外是苏丹，该国提交的两份材料中涉及的内容是其他材料中没有的。一份材料提到，美国对苏丹的政治制裁是对互联网中立性的破坏。另一份提到，互联网名称与数字地址分配机构是美国政府操纵的机构，它会给苏丹这样遭受美国制裁国家的信息自由流动造成不利影响。

第三，非洲网络安全治理的能力建设亟需加强。受到资金和技术能力限制，非洲国家打击网络犯罪的机构和人员配置不足，给制度安排的落实带来了障碍。非洲国家负责互联网安全的多是信息通讯技术部门，且没有类似中国网信办、美国白宫网络安全协调人这样的专门机构、人员设置。非盟层面也缺乏像“欧洲网络与信息安全局”（ENISA）这样的机构，后者专门负责组织、协调欧盟各成员国信息安全战略规划、实践、基础设施保护和应急响应等工作。

第四，在网络安全治理方面，非盟和成员国、官方和非官方尚未形成合力。值得非洲国家借鉴的是，欧盟已经形成了以“一个主题（网络安全）、两个层面（欧盟和成员国）、3 个主体（政府部门、私营企业、学术界）”为特征的网络安全管理体制，并在不同层面和不同主体之间初步建立起一套信息共享机制。[②] 与欧洲相比，非洲的一体化程度要低很多，非盟和成员国的关系也不是十分紧密，非盟难以发挥欧盟那样的统筹、协调作用，非洲国家集体行动应对网络威胁的能力也面临挑战。此外，非洲非政府组织发展不太成熟，

---

① Ephraim Percy Kenyanito, “Spotlight on African Contributions to Internet Governance Discussions (Part 1: NETmundial)”, April 23, 2014, http://www.circleid.com/posts/20140423_african_contributions_to_internet_governance_discussions_part_1, 2015-06-19.

② 雷小兵、黎文珠：《〈欧盟网络安全战略〉解析与启示》，载《信息安全与通信保密》2013 年第 239 期，第 56～57 页。

多数受到了西方国家或互联网公司的支持，所倡导的也是“自由”、“民主”等西方的核心价值观，与非洲各国政府的核心关切不是十分契合，这也使非洲难以形成“官方与非官方渠道相结合”的治理模式。

A Primary Exploration on Cyber Security Governance in Africa

Xiao Yingying & Yuan Zhengqing

Abstract: The internet history in Africa is short, but this new technology is spreading fast on the continent. Along with these, cybercrime in Africa is becoming increasingly rampant, while the relevant legal institutions and law enforcement capacity are lagging behind, with public and private cyber security awareness being relatively weak, etc. Besides e - transaction and cybercrime, personal data protection is also part of Africa's cyber security governance, which is the result of the "teaching" from developed countries in the western world and the active advocacy from NGOs. Whether at the national level, sub - regional organization level, African Union level or NGO level, those developed countries of the western world and western - dominated international organizations have played a role in the institutional design of African cyber security governance, some of which referred to or even copied the original designs of the western world. This may lead to the African continent being re - colonized in cyberspace, with no autonomous decision - making power in global cyber security governance. Besides, from design to implementation, African countries still have a long way to go, and whether the institutions based on the western experience are suitable for the culture and ideas of the African countries, remains to be tested by practice.

Key Words: Cyber Security; Cyber Crime; Data and Privacy Protection; Governance Approach; AU

（责任编辑：詹世明　责任校对：樊小红）