区域动态（撒哈拉以南非洲）

目录

专题聚焦

非洲电信网络诈骗：类型、影响与对策

在非洲，数字经济的迅猛发展正在深刻改变当地的生活方式和经济结构。得益于互联网和信息通信技术（ICT）的迅速普及，非洲的数字经济正在经历空前的增长。数字经济在推动非洲经济增长的过程中扮演了不可或缺的角色。在这个数字化日益重要的时代，国际贸易对非洲经济的促进作用越发依赖于数字经济的发展。因此，为了最大限度地利用国际贸易的经济潜力，非洲各国政府都在努力发展本国的数字经济。

然而，数字经济的繁荣背后，电信网络诈骗问题也日益严重。著名信息安全领导厂商“卡巴斯基实验室”（Kaspersky）表示非洲正成为网络攻击的新目标。与此同时，国际刑警组织（Interpol）在 2023 年发布的《非洲网络威胁评估报告》（African Cyberthreat Assessment Report 2023）中明确指出，电信网络诈骗已成为非洲大陆面临的最普遍威胁之一。

在当前全球经济低迷和新冠疫情的双重打击下，非洲多个国家的产业面临重大挑战，这种困境加剧了电信网络诈骗的泛滥。越来越多失业或破产的人群，因高收入工作或高收益融资的诱惑而易受欺骗。这些因素共同促使非洲电信诈骗问题日益严重。鉴于此，深入了解和分析非洲国家的电信网络诈骗现象显得尤为重要。本文将首先详细分析非洲电信网络诈骗的多种类型及其采用的手段，并通过具体案例来揭示其复杂性和危害性。接下来，文章将探讨这种诈骗对非洲各国经济、社会、政治等多个方面的深远影响，以及这些诈骗活动如何利用和放大现有的社会经济问题。然后，我们将评估非洲国家在打击电信网络诈骗方面所采取的策略和措施。最后，文章将总结当前的情况，并对未来非洲电信网络诈骗的发展趋势及可能的解决方案进行展望。

一、 非洲电信网络诈骗的类型与手段

电信网络诈骗是指犯罪分子通过电话、网络和短信等方式，编造虚假信息，设置骗局，对受害人实施远程、非接触式诈骗，诱使受害人给犯罪分子打款或转账的犯罪行为。2023 年 3 月，国际刑警组织非洲网络犯罪行动办公室发布非洲七大网络诈骗类型，包括商业电子邮件欺诈（Business Email Compromise，BEC）、网络钓鱼（Phishing）、勒索软件攻击（Ransomware）、银行木马与盗窃（Banking Trojans and Stealers）、网络诈骗（Online Scams）、网络勒索（Cyber Extortion）、犯罪软件即服务（Crimeware-as-a-Service）。同年 6 月，中国公安部公布国内十大电信网络诈骗类型，包括刷单返利类诈骗，虚假网络投资理财类诈骗，虚假网络贷款类诈骗，冒充电商物流客服类诈骗，冒充公检法类诈骗，虚假征信类诈骗，虚假购物、服务类诈骗，冒充领导、熟人类诈骗，网络游戏产品虚假交易类诈骗以及婚恋、交友类诈骗。相比较而言，国际刑警组织的分类倾向于突出技术层面和国际化的网络犯罪特征，而中国公安部的分类则更偏重于国内公众的教育和防范。但就本质上来说，这些都是对犯罪行为模式、技术特征和社会影响的细致划分。在上述诈骗类型中，商业电子邮件欺诈、网络

钓鱼和勒索软件攻击在非洲尤为突出，它们共同构成了非洲数字安全的主要威胁。因此，深入研究这些诈骗类型，了解它们的运作机制和防范措施，对于认识非洲国家的数字经济和数字安全来说至关重要。

非洲电信网络诈骗的复杂性根源于其多样的手段和策略，这种多样性在其地理和文化的多元性中得到了充分体现。虽然非洲的电信网络诈骗正在迅猛发展，但非洲拥有 54 个国家，难以在一篇文章详尽地阐述问题所在。在同时考虑时间和空间的前提下，本文从非洲西部、非洲东部和非洲南部分别挑选了尼日利亚、肯尼亚和南非作为案例，时间跨度为 20 世纪 80 年代至 21 世纪 20 年代。尼日利亚的商业电子邮件欺诈、肯尼亚的网络钓鱼和南非的勒索软件攻击，都是非洲国家目前在电信网络诈骗领域中面临的主要问题。对这些具有代表性的案例进行深入分析，有助于理解非洲电信网络诈骗的特殊性和挑战性，并为全球范围内的防范和应对策略提供重要的视角。

图 1：非洲正在遭受电信网络诈骗

https://techcabal.com/2022/05/06/africa-cybercrime-cyber-africa-forum/

（一） 尼日利亚：商业电子邮件欺诈

作为非洲第一大经济体，尼日利亚在人口数量、地理位置和 ICT 基础设施等方面存在明显优势，有望成为非洲数字经济的领军者。然而，在数字经济的日益繁荣背后，尼日利亚面临着电信网络诈骗带来的严重威胁。尼日利亚的电信网络诈骗历史悠久，早在 20 世纪 80 年代就已存在，其中最著名的诈骗方式之一是网络钓鱼。当时，就出现了一些冒充“尼日利亚王子”的骗子，他们在西方国家掀起了一场电信网络诈骗风暴，给当地人造成了巨大的经济损失。由于其广泛的影响，这种诈骗方式甚至被命名为“尼日利亚王子骗局”。近年来，更为复杂的商业电子邮件欺诈在全球范围内泛滥，尼日利亚也未能幸免。

在商业电子邮件欺诈中，诈骗犯通常未经授权访问企业电子邮件账户，利用这些账户向

业务伙伴发送欺诈性信息，诱使他们转账或泄露敏感信息。虽然各界对这一行为的定义存在差异，但普遍认为其本质是“通过发送冒充供应商或业务合作伙伴的欺骗性电子邮件来欺骗企业进行汇款的骗局”。根据 IBM《2023 年度数据泄露成本报告》（Cost of a Data Breach Report 2023）的数据，商业电子邮件欺诈造成的平均损失为 498 万美元。尼日利亚的诈骗犯采用精心策划的手段，伪装成目标员工的同事、供应商、合作伙伴或客户发送电子邮件。这些电子邮件的目的是诱骗员工支付欺诈性发票、向虚假银行账户进行电汇或者泄露客户数据、知识产权或公司财务等敏感信息。为了提高诈骗的可信度，这些犯罪分子会深入研究目标员工的背景，以及他们所冒充的人物的身份特征。他们利用社会工程学技术，制作仿佛是真实发件人所发送的欺骗性电子邮件。在某些情况下，他们实际上会侵入并劫持发件人的电子邮件帐户，从而使攻击电子邮件更加可信，甚至与合法电子邮件几乎无法区分。他们通常将焦点放在富裕的西方国家，这或许是因为尼日利亚过去是英国殖民地。此外，他们往往选择的是那些拥有典型西方名字的平民，如约翰（John）、迈克尔（Michael）、安妮（Anne）、莎拉（Sarah）、玛丽（Mary），而不常针对东欧国家的居民，这一选择偏好可能源于他们对英语使用者的熟悉度和攻击的便利性。诈骗者常伪装成来自欧洲或美洲的专业人士，涉及的职业包括工程师、跨国公司高层、军官、船长等，以提高其诈骗的可信度和效果。

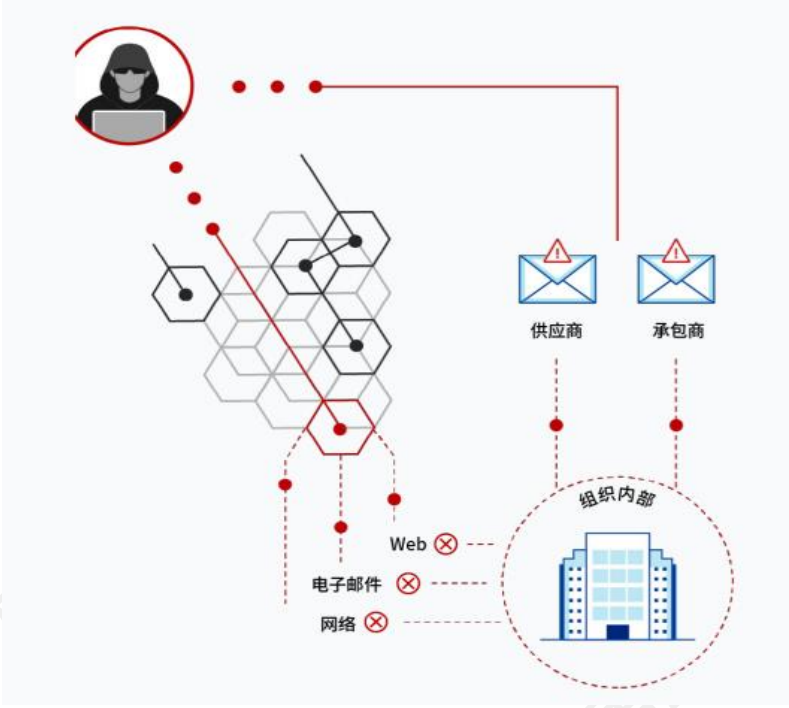

图 2：商业电子邮件欺诈的流程图

https://cf-assets.www.cloudflare.com/slt3lc6tev37/4sivQSVRKbmDGL6VqSLLmM/2204135e3f84dc565652cae0f809f50a/Whitepaper_Area-1-How-to-Stop-Business-Email-Compromise-Threats_Simplified-Chinese_20220921.pdf

（二） 肯尼亚：网络钓鱼

国际咨询公司 Dalberg 的《肯尼亚的数字经济：民众的视角》（Kenya's Digital Economy: A People's Perspective）报告表示，通过对肯尼亚 2456 名 15 岁以上居民的访谈调查发现，该国互联网渗透率为 65%，手机普及率为 98%，移动支付覆盖率为 94%，这些数据显示肯尼亚在非洲的数字经济发展中占据领先地位。然而，这一快速发展的背后，肯尼亚面临着一个严峻的挑战——电信网络诈骗。尤其是网络钓鱼，已成为威胁其数字经济发展的主要问题。

在网络钓鱼中，诈骗犯诱使用户下载恶意软件、共享敏感信息或个人数据（例如社会保险号和信用卡号、银行账号、登录凭据）。这种攻击通常包含三个步骤：发送钓鱼邮件、受害者接收邮件、受害者按邮件指示采取行动。根据 IBM《2023 年度数据泄露成本报告》（Cost of a Data Breach Report 2023）的数据，网络钓鱼造成的平均损失为 476 万美元。肯尼亚的诈骗犯通常伪装成受害者信任的人或组织，并造成一种紧迫感，促使受害者鲁莽行事。这种策略之所以流行，是因为相较于直接入侵计算机或网络，欺骗用户既简单又成本低。2022 年上半年，肯尼亚遭受的电信网络诈骗数量急剧增加，网络钓鱼的数量同比增长了 438%。根据环联（TransUnion）在《2023 年全渠道诈骗状况报告》（2023 State of Omnichannel Fraud）中的数据，59%的肯尼亚人认为网络钓鱼是最令人担忧的电信网络诈骗类型。金融机构是网络钓鱼的主要受害者，自 2019 年以来，该领域的未遂案件增加了 309%，这一现象主要归因于数字技术的快速发展和在线交易量的增加。

图 3：网络钓鱼的流程图

http://www.360doc.com/content/22/0817/01/37113458_1044172822.shtml#google_vignette

（三） 南非：勒索软件攻击

南非在数字经济方面有巨大的发展潜力。南非在互联网使用率（54%）、移动电话普及率（80%）和宽带覆盖率（99%）等指标上处于非洲地区领先地位。但良好的数字经济基础也为电信网络诈骗的发展提供了滋生的土壤。自 2019 年起，在南非出现的各类电信网络诈骗已引发社会关注。中国驻南非使领馆于 2019 年、2021 年、2022 年和 2023 年均发布安全提示，要求在南非旅行或从事其他事务的中方人员谨防南非地区出现的电信网络诈骗犯罪，以免造成经济损失。近年来，勒索软件攻击在南非显著增加，对企业和政府机构构成了严重威胁。

在勒索软件攻击中，诈骗犯锁定受害者的数据或设备，并威胁受害者，使其保持锁定状态，并要求受害者向攻击者支付赎金。根据 IBM 的《X-Force 威胁情报资料指数报告》（X-Force Threat Intelligence Index），勒索软件攻击占 2022 年网络攻击总数的 17%。南非的诈骗犯起初只是要求通过支付赎金换取重新访问受影响数据或使用受感染设备所需的加密密钥。后来，诈骗犯不仅加密受害者的数据，还窃取数据，并威胁要公开这些信息，除非支付更高的赎金。再后来，又出现了三重勒索攻击，这种攻击形式不仅包括数据加密和窃取，还可能涉及对受害者客户或合作伙伴的额外勒索。根据安全威胁监控平台 Shadowserver 的数据，2022 年 1 月至 9 月间，非洲是勒索软件攻击的主要目标地区之一，其中南非尤为突出，占所有检测到的案例的 42%。这类攻击不仅导致重大经济损失，还可能对企业的运营造成严重干扰。例如，2021 年 9 月，南非司法部遭受勒索软件攻击，导致所有电子服务瘫痪。2023 年 8 月，Snatch 勒索软件组织声称将对南非国防部网络主机发起攻击。这些事件不仅导致了数据和服务的损失，也对公共信任造成了影响。勒索软件攻击的频繁发生揭示了南非在网络安全方面的薄弱环节，尤其是在系统安全和网络防护方面。

图 4：勒索软件攻击的流程图

https://www.infosec.gov.hk/sc/knowledge-centre/ransomware

二、 非洲电信网络诈骗的多维度影响

非洲的电信网络诈骗现象是一个复杂且多维度的问题，其影响范围远超出单纯的经济损失。这种诈骗活动不仅扰乱了市场秩序，影响了数字经济体系的健康发展，而且在社会、政治层面上造成了深远的影响。在社会层面上，它破坏了社会诚信基础，损害了公民的隐私和安全，引发了社会不满和动荡。在政治层面上，这些活动损害了非洲国家的国际形象，削弱了公众对政府的信任，并对法律体系和治理能力提出了挑战。此外，非洲电信网络诈骗呈现出专业化、集团化和国际化的特点，反映出其个性与全球电信网络诈骗的共性相互交织的复杂性。

（一） 经济影响

非洲的电信网络诈骗不仅给受害者造成了直接的经济损失，更对整个数字经济体系产生了深远的影响。首先，这些诈骗活动扰乱了市场的正常运作，严重破坏了商业信誉环境。由于诈骗行为的普遍性，企业和消费者在进行交易时变得更加谨慎和怀疑，这不仅增加了交易的复杂性，还提高了交易成本。以尼日利亚为例，根据尼日利亚通信委员会（NCC）2020 年的报告，电信网络诈骗的激增对市场秩序造成了严重影响，导致约 125 亿奈拉的经济损失。这种破坏性影响对市场经济的持续健康发展构成长期威胁。其次，电信网络诈骗给个人和企业造成了严重的经济损失。许多人因为电信网络诈骗而遭受重大财务损失，甚至倾家荡产。例如，2022 年上半年，肯尼亚遭受的电信网络诈骗数量急剧增加，网络钓鱼事件的数量同比增长了 438%。这些损失不仅包括个人直接的金钱损失，还有企业为预防未来诈骗所增加的安全投资和运营成本。最后，这种犯罪活动破坏了数字市场的整体信任和安全感。在数字经济中，对数字平台的信任是至关重要的。电信网络诈骗的增加导致消费者和企业对在线交易持怀疑态度，这不仅阻碍了数字经济的发展，还使外部投资者因对市场的不信任而犹豫投资，进一步对非洲国家的经济发展构成了长期威胁。

（二） 社会影响

电信网络诈骗在非洲的蔓延，尤其是在尼日利亚、肯尼亚和南非等国，构成了一个多维度的挑战，其影响远超经济层面，深刻侵蚀着社会的信任和安全感。首先，在社会层面，这种诈骗活动严重损害了社会的诚信基础，影响了社会和谐与稳定。尼日利亚近年来在国际上因电信网络诈骗而声名狼藉。一些执法机构能够追踪到部分诈骗案件的源头在尼日利亚，这导致该国成为被指责的焦点。这种负面形象对普通的尼日利亚公民产生了不利影响。例如，许多尼日利亚人出国是为了学习或进行合法的商业交易，但他们常常因此而不得不接受更加严格的安全检查。其次，电信网络诈骗还可能导致个人信息的泄露，严重影响公民的隐私和安全。个人信息的滥用不仅侵犯了个人隐私，还可能导致进一步的诈骗和身份盗用，使受害者陷入更大的困境。同时，电信网络诈骗的增加也反映出监管框架和法律体系的不足。最后，电信网络诈骗的猖獗不仅给受害者带来深刻的痛苦，还给执法部门带来了重大的负担。这导致了公共资源和注意力的分散，影响了对其他重大犯罪的打击和预防工作。

（三） 政治影响

电信网络诈骗不仅仅会危害个人和企业的经济利益，侵蚀着社会的信任和安全感，也会破坏所在国的国家形象，甚至引发国家之间的纠纷和外交摩擦，进而破坏国家间的信任和合作关系。首先，对于非洲国家，特别是尼日利亚，频繁发生的电信网络诈骗已严重损害了其国际形象。这种负面形象可能影响国家间的外交关系，降低外国投资者对这些国家的信心。这种负面影响不仅限于经济领域，更可能波及到政治的层面。其次，电信网络诈骗的增加导致公众对政府保护其免受网络犯罪的能力产生怀疑。这种怀疑不仅削弱了民众对政府的信任，还可能激发社会不满和动荡。当公民感到他们的个人信息和经济安全受到威胁时，对政府的支持和信任可能会降低。最后，电信网络诈骗的增加对非洲国家的法律体系和治理能力提出了挑战。例如，南非政府近年来加大了对网络犯罪的打击力度，但由于缺乏足够的技术专业知识和国际合作，其效果仍有限。

图 5：非洲国家正加大打击电信网络诈骗的力度

https://www.unodc.org/westandcentralafrica/en/westandcentralafrica/stories/2022/how-to-combat-cyber-organized-crime-in-west-africa.html

事实上，非洲电信网络诈骗的现象不仅体现了全球电信网络诈骗的普遍特点，而且展现了其特有的个性特征。首先，非洲电信网络诈骗具有专业化、信息化的趋势，犯罪手段趋向于复杂和多元。诈骗犯通常拥有严密的组织结构，分工明确，其中包括技术支持人员和实际操作人员，每个环节都有专责人员执行。他们利用现代信息技术，如电脑和电话，通过互联网服务器执行大规模的短信群发和电话拨打，以诱导受害人将资金转入指定账户。其次，非洲电信网络诈骗正在呈现集团化、产业化的特点，存在与武装组织和贪腐官员勾结的问题。这些诈骗团伙通常由分工明确、组织严密的成员组成，表现出显著的集团化特征。他们中的

一些散布在非洲国家的边远山区，甚至与某些武装组织有联系，或者通过贿赂当地官员来寻求保护。再次，非洲国家电信基础设施薄弱，配套的法律制度保障不足，安全防护能力明显不足。在互联网迅速普及的当下，非洲的网络安全防护能力并未能同步增长，从而在网络空间留下了许多漏洞和安全隐患。这为不法分子提供了可乘之机，使得电信网络诈骗活动在非洲国家易于蔓延且难以根除。最后，随着非洲电信市场逐渐与世界接轨，电信网络诈骗的国际化特征愈发明显。特别是在亚洲地区打击电信网络诈骗力度加大后，原本集中在亚洲的诈骗犯开始向非洲转移。结合非洲本土的诈骗集团，电信网络诈骗呈现出全球化的趋势，其受害者不再局限于单一国家，而是扩散到全球范围。综上所述，非洲电信网络诈骗的复杂性是其个性与全球电信网络诈骗的共性相互交织的结果。

三、 非洲电信网络诈骗的应对举措

面对全球范围内日益增长的电信网络诈骗威胁，非洲国家和国际社会正积极采取行动以应对这一挑战。本章节将深入探讨三个关键层面的策略：首先是非洲国家在本国层面的策略，如尼日利亚成立专门机构打击经济犯罪，肯尼亚加强网络安全基础设施以及南非实施严格的个人信息保护法律；其次是国际合作，包括多国联合执法行动和区域合作组织在内的合作机制；最后是国际组织的支持，特别是国际刑警组织与当地执法部门的合作，以及网络安全公司在打击电信网络诈骗中的作用。

（一） 所在国的策略

为了应对电信网络诈骗，2004 年尼日利亚成立了经济与金融犯罪委员会（EFCC），专注于打击国内的经济犯罪。近年来，该组织在打击“雅虎男孩”（Yahoo Boys）[1]上取得了一定的成效。在打击商业电子邮件欺诈方面，经济与金融犯罪委员会主要与其他国家的执法机构合作，以逮捕和引渡涉嫌犯罪的尼日利亚公民。肯尼亚为打击网络钓鱼采取了一系列举措，以加强网络安全基础设施，其中包括建立国家网络安全局和国家计算机事件响应小组（National KE-CIRT/CC），该机构自 2017 年 8 月起开始全天候运营，配备了最先进的系统，以检测、分析国家网络威胁，调查网络犯罪。2018 年 5 月，肯尼亚颁布《计算机滥用和网络犯罪法》（Computer Misuse and Cybercrimes Act），定义了与计算机系统有关的犯罪行为，旨在及时发现、禁止、预防、调查和起诉网络犯罪，并加强在打击电信网络诈骗方面的国际合作。2020 年 11 月，肯尼亚通信与技术部长乔·穆切鲁（Joe Mucheru）强调，除了政府外，企业也需制定并推行自己的措施来遏制网络威胁。为了应对勒索软件攻击，南非国家运输集团 Transnet 采取了紧急措施。员工被指示关闭所有连接到其网络和域的设备，并避免从手机访问电子邮件或在 MS Teams 上进行会议。南非的《个人信息保护法案》（POPIA）对企业提出了具体要求，以维护其处理的信息的完整性和保密性。这包括采取技术和组织措

[1] 多用于指代尼日利亚借助“雅虎免费邮箱”进行电信诈骗的人群。

施防止非法访问其控制的信息。当企业成为勒索软件攻击的受害者时，它们需履行包括通知数据主体、信息监管机构和南非警察局等相关方的多项义务。

（二） 国家间的合作

鉴于商业电子邮件欺诈的普遍性及网络空间的复杂性，尼日利亚政府正寻求通过国际合作加强打击网络犯罪的力度。利用《司法互助协定》（Mutual Legal Assistance Treaty）等多边条约，尼日利亚有望在网络犯罪调查、证据收集和网络安全领域得到其他国家的支持和协助。比如，2019 年，美国和尼日利亚联合发动“reWired 行动”，专门打击商业电子邮件欺诈，最终逮捕了 281 名嫌疑人，涉及美国、尼日利亚、土耳其、加纳、法国、意大利、日本、肯尼亚、马来西亚和英国等多个国家。此次国际行动查获了近 370 万美元，并且中断和追回了约 1.18 亿美元。东非国家通过政府、行业和民间社会组织等多方利益相关者的方式加大力度打击网络犯罪。由肯尼亚领导的网络安全管理工作组（Computer Emergency Response Teams，CERTs）一直在协调旨在根除东非共同体五个成员国的网络犯罪的活动。该工作组负责法律、政策和监管层面的网络安全。此外，肯尼亚成立的国家网络安全局和国家计算机事件响应小组不仅在本国范围内发挥作用，而且与地区和国际相关行为者合作，强化了网络安全的全球联动机制。这些努力展示了非洲国家在网络安全领域日益增强的区域和国际合作，以及对抗日益复杂的网络威胁的决心。

（三） 国际组织的支持

近年来，尼日利亚的商业电子邮件欺诈已成为全球网络犯罪的一个重要部分，为了应对这一挑战，尼日利亚警察部队（NPF）与国际刑警组织展开了紧密合作。他们的目标是捣毁在该地区活动的电信网络诈骗团伙，尤其是名为 Silver Terrier 的电信网络诈骗巨头。Silver Terrier 被认为是一系列复杂的电子邮件诈骗活动的幕后主导者，这些活动不仅对尼日利亚，也对全球造成了巨大的经济损失。2022 年 5 月，国际刑警组织与网络安全公司 Group-IB、Palo Alto Networks 和 Trend Micro 开展合作，成功发动了“Delilah 行动”，共同打击尼日利亚的电信网络诈骗。“Delilah 行动”完成后，“Killer Bee 行动”也随之开展，突显了在打击跨国网络犯罪方面的国际合作的重要性。这两次行动有效地阻止了商业电子邮件欺诈，并对全球网络犯罪圈产生了震慑效应。国际刑警组织和尼日利亚警察部队在这些行动中的合作体现了跨国网络犯罪打击的新趋势。通过将国际执法资源与私营部门的技术专长结合起来，这种模式在全球范围内为打击电信网络诈骗提供了一个新的方向。此外，这些行动也展示了网络安全公司在当代网络犯罪打击中的重要作用。Group-IB、Palo Alto Networks 和 Trend Micro 等公司不仅提供了先进的技术支持，还提供了关键的情报信息，帮助执法机构更有效地定位和打击犯罪团伙。

图 6：国际刑警组织打击非洲电信网络诈骗

https://www.interpol.int/News-and-Events/News/2021/INTERPOL-launches-initiative-to-fight-cybercrime-in-Africa

结语

本文深入分析了非洲面临的电信网络诈骗问题，重点关注商业电子邮件欺诈、网络钓鱼和勒索软件攻击等类型。这些诈骗行为不仅给非洲国家带来经济损失，还在社会和政治层面造成了严重影响：破坏了社会信任，侵犯了公民隐私与安全，损害了国家的国际形象，削弱了公众对政府的信任，并对法律体系和治理能力提出了挑战。文章详细讨论了非洲国家采取的策略，包括在国内层面成立专门机构、加强网络安全基础设施、实施个人信息保护法律等。此外，文章还强调了国际合作的重要性，包括跨国执法行动和区域合作组织的作用，以及国际组织如国际刑警组织与当地执法部门的合作。通过这些措施，非洲国家与国际社会共同努力，旨在有效应对和减少电信网络诈骗带来的威胁。

展望未来，非洲电信网络诈骗的发展态势将由技术进步和国际合作共同塑造。随着数字技术的快速发展，诈骗手段预计将变得更加精细和难以识别，对公众和企业的威胁亦随之增加。然而，这也为非洲国家提供了利用先进技术和增强国际合作来有效打击电信网络诈骗的机遇。未来的关键将在于如何平衡这些挑战和机遇。

资料来源

[1]. Abendin, S., & Duan, P. (2021). International trade and economic growth in Africa: The role of the digital economy. *Cogent economics & finance*, *9*(1), 1911767.

[2]. Adeyemi Adepetun, "Combating telecoms-related electronic frauds in Nigeria", June 2023, https://guardian.ng/technology/combating-telecoms-related-electronic-frauds-in-nigeria/, (accessed January 15, 2024).

[3]. Adeyemi Adepetun, "Cybercrime rises as phishing hits 174% in Nigeria, 438% in Kenya", August 2022, https://guardian.ng/business-services/cybercrime-rises-as-phishing-hits-174-in-nigeria-438-in-kenya/, (accessed January 17, 2024).

[4]. Burrell, J. (2008). Problematic empowerment: West African Internet scams as strategic misrepresentation. *Information Technologies & International Development*, *4*(4), pp-15.

[5]. FBI, "Worldwide Sweep Targets Business Email Compromise", September 2019, https://www.fbi.gov/news/stories/operation-rewired-bec-takedown-091019, (accessed January 15, 2024).

[6]. Fredrick Obura, "Kenya steps up fight against cybercrime", Novembre 2020, https://www.standardmedia.co.ke/business/sci-tech/article/2001393164/kenya-steps-up-fight-against-cybercrime, (accessed January 15, 2024).

[7]. Friederici, N. (2018). *Hope and hype in Africa's digital economy: The rise of innovation hubs*. Boston, MA: MIT Press.

[8]. Glickman, H. (2005). The Nigerian "419" advance fee scams: prank or peril?. *Canadian journal of African studies/La revue canadienne des études africaines*, *39*(3), 460-489.

[9]. Grabosky, P., & Smith, R. (2003). Telecommunication fraud in the digital age: The convergence of technologies. In *Crime and the Internet* (pp. 41-55). Routledge.

[10]. Grobler, M., & van Vuuren, J. J. (2010, August). Broadband broadens scope for cyber crime in Africa. In *2010 Information Security for South Africa* (pp. 1-8). IEEE.

[11]. IBM, "Cost of a Data Breach Report 2023", August 2023, https://www.ibm.com/cn-zh/reports/data-breach, (accessed January 17, 2024).

[12]. IBM, "IBM Security X-Force Threat Intelligence Index 2023", https://www.ibm.com/reports/threat-intelligence, (accessed January 17, 2024).

[13]. Ihuoma Chiedozie, "Nigeria'll become Africa's leading digital economy, says minister", 28 October 2019, https://punchng.com/nigeriall-become-africas-leading-digital-economy-says-minister/, (accessed January 11, 2024).

[14]. Intelpol, "African Cyberthreat Assessment Report 2023", March 2023, https://www.interpol.int/content/download/19174/file/2023_03%20CYBER_African%20Cyberthreat%20Assessment%20Report%202022_EN.pdf, (accessed January 10, 2024).

[15]. Karl Blom and Laone Setshedi, "Ransomware attacks: how South African companies should respond", November 2023, https://techcentral.co.za/ransomware-attacks-south-african-respond/234661/, (accessed January 15, 2024).

[16]. Kehinde Oyedeji, J., & Olamide Badmos, H. (2022). Social construction of internet fraud as innovation among youths in Nigeria. *International Journal of Cybersecurity Intelligence & Cybercrime*, *5*(1), 23-42.

[17]. Koi-Akrofi, G. Y., Koi-Akrofi, J., Odai, D. A., & Twum, E. O. (2019). Global telecommunications fraud trend analysis. *International Journal of Innovation and Applied Studies*, *25*(3), 940-947.

[18]. Longe, O., Ngwa, O., Wada, F., Mbarika, V., & Kvasny, L. (2009). Criminal uses of information & communication technologies in sub-Saharan Africa: trends, concerns and perspectives. *Journal of Information Technology Impact*, *9*(3), 155-172.

[19]. Natassia Badenhorst, "Vishing, Smishing and Phishing Are the Top Types of Fraud in Kenya, According to TransUnion", May 2023, https://newsroom.transunionafrica.com/vishing-smishing-and-phishing-are-the-top-types-of-fraud-in-kenya-according-to-transunion/, (accessed January 17, 2024).

[20]. Okpa, J. T., Ajah, B. O., Nzeakor, O. F., Eshiotse, E., & Abang, T. A. (2023). Business e-mail compromise scam, cyber victimization, and economic sustainability of corporate organizations in Nigeria. *Security Journal*, *36*(2), 350-372.

[21]. Quarshie, H. O., & Martin-Odoom, A. (2012). Fighting cybercrime in Africa. *Computer Science and Engineering*, *2*(6), 98-100.

[22]. Republic of Kenya , "Kenya Gazette Supplement", May 2018, kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ComputerMisuseandCybercrimesActNo5of2018.pdf, (accessed January 17, 2024).

[23]. Ridwaan Docrat, "Ransomware Attacks in South Africa: What You Need to Know", June 2023, https://isite.co.za/ransomware-attacks-south-africa/ , (accessed January 15, 2024).

[24]. 肖莹莹,袁正清.非洲网络安全治理初探[J].西亚非洲,2016,(03):121-137.

[25]. 新浪财经，《金砖各国处于数字经济高速发展期》，2022 年 7 月 4 日，https://finance.sina.com.cn/tech/2022-07-04/doc-imizmscu9980881.shtml?finpagefr=p_114，（访问时间：2024 年 1 月 17 日）

[26]. 中国新闻网，《公安部公布十大高发电信网络诈骗类型》，2023 年 6 月 15 日，https://www.chinanews.com.cn/gn/2023/06-15/10025282.shtml，（访问时间：2024 年 1 月 13 日）

各国动态

刚果（金）

【政治动态】刚果（金）总统齐塞克迪在质疑声中赢得连任

当地时间 2023 年 12 月 31 日，刚果（金）国家独立选举委员会公布总统选举初步计票结果，现任总统齐塞克迪赢得新一届总统选举，赢得连任。据官方数据，齐塞克迪在 12 月 20 日举行的总统、议会和地方选举中获得了 73.34%的选票，远超其他候选人。加丹加省前省长卡通比以 18.08%的选票位居第二，为公民和发展而战斗党（ECiDé）领导人法尤卢则以 5.33%的选票位列第三。选举委员会透露，本次选举的投票率大约为 43%。根据刚果（金）的选举日程，宪法法院计划于 2024 年 1 月 10 日宣布选举的最终结果。新当选的总统预计将在 1 月 20 日宣誓就职。然而，选举结果公布后，多名反对派总统候选人对选举的公正性提出质疑。

——编译自 12 月 31 日 *The New York Times*

埃塞俄比亚

【政治动态】埃塞俄比亚与索马里兰签署谅解备忘录

当地时间 1 月 1 日，埃塞俄比亚与非洲东部的索马里兰在埃塞首都亚的斯亚贝巴签署谅解备忘录。根据该备忘录的内容，埃塞俄比亚将获得索马里兰港口的使用权，并且或将承认索马里兰的独立。这一决定标志着埃塞俄比亚可能成为首个正式承认索马里兰独立的国家。官方表示，此次合作与伙伴关系的备忘录旨在开启双方在多个领域的合作。作为对这一事件的回应，索马里政府于次日宣布召回其驻埃塞俄比亚大使。

——编译自 1 月 1 日 *The Guardian*

塞内加尔

【经济动态】塞内加尔化肥价格飙升引发危机

近期，塞内加尔的化肥价格激增，暴露出非洲国家在面对全球市场波动时的脆弱性。自新冠疫情爆发以来，全球化肥供应链受到挑战，俄乌冲突导致的全球能源价格飙升间接影响了能源作为重要成本的化肥产业。同时，俄罗斯作为主要化肥生产国之一，其不稳定的供应对非洲国家造成了显著影响。此外，美元兑当地货币走强，加剧了非洲的进口成本。具体而

言，2022 年初至 2023 年初，塞内加尔的化肥价格翻了一番。塞内加尔政府尝试通过补贴稳定市场，但由于管理不善，这些措施收效甚微。

——综合编译自 1 月 5 日 *Le Monde*

非洲

【科技动态】联合国人工智能专家警告非洲或将面临“数字殖民”

当地时间 1 月 3 日，联合国人工智能高级别咨询机构专家塞迪娜·穆萨·恩迪亚耶对非洲国家在人工智能领域的发展提出警告。恩迪亚耶指出，尽管人工智能技术为非洲带来了便利，但如果放任其无序发展，非洲可能会进一步失去在科技领域的自主性。他强调，目前非洲在人工智能技术方面主要依赖国外公司，而不是本土企业。恩迪亚耶进一步说明，如果人工智能的解决方案继续由外国公司主导并强加给非洲国家，那么非洲将面临人工智能发展中的一个巨大威胁，即“数字殖民”。

——编译自 1 月 3 日 *Africa Renewal*

南非

【政治动态】南非与摩洛哥争夺联合国人权理事会主席

当地时间 1 月 9 日，南非和摩洛哥在联合国最高人权机构主席人选问题上发生争执，南非称摩洛哥在西撒哈拉犯下了侵犯人权的罪行，不具备领导该机构的能力与信誉。两个非洲国家公开在联合国人权理事会进行争论，此举极为罕见。次日，摩洛哥常驻日内瓦代表兹尼贝尔大使获得 30 票，南非常驻日内瓦代表恩科西大使获得 17 票，最终摩洛哥赢得联合国人权理事会主席的席位。

——编译自 1 月 10 日 *Reuters*

编译：卜现东

校对：撒哈拉以南非洲组