THE LINUX FOUNDATION | Research

携手应对共同挑战

2023 年开源大会报告

Anthony Williams, 总裁兼联合创始人, DEEP Centre
前言：陈岳和 Chris Xie, Futurewei Technologies 公司

2023 年 12 月

由

FUTUREWEI Technologies

赞助

信息图

携手应对共同挑战

作为人类的集体知识库，开源基于透明、包容和社区驱动开发等核心原则而蓬勃发展。

携手应对共同挑战

要保持开源的韧性，就需要整个社区致力于应对网络安全、人工智能（AI）和技术民族主义等共同挑战。

携手应对共同挑战

开源软件的安全性取决于健康的网络安全专业人才库，以及吸引和留住维护者的激励机制。

携手应对共同挑战

开源社区应采用"默认安全"模式，将安全性作为应用程序设计的基础。

携手应对共同挑战

开源软件的普及使得监管审查持续增加，因此对政策制定者的宣导和教育至关重要，以确保新的法规与开源原则和实践能相互兼容。

携手共同应对挑战

开源基金会必须利用其法律敏锐性、沟通和社区参与技能，在政策领域进行有效宣传。

携手共同应对挑战

数字主权措施可能会增加碎片化，阻碍监管协调，但各国促进技术自主的努力也导致了更多开源的采用。

携手共同应对挑战

基金会可以通过建立中立的协定来管理社区贡献，保持知识和技术的跨境流动，从而缓解地缘政治紧张局势。

携手共同应对挑战

社区可以通过致力于多样性和包容性以及利用行为准则来促进共同规范，从而吸引新的人才并最大限度地发挥其社会影响。

携手共同应对挑战

可解释性和来源出处对于提高人工智能系统的可信度以及解决许可、安全和治理问题至关重要。

携手共同应对挑战

要管理与日益强大和普及的人工智能系统相关的新风险和伦理问题，透明度和公开性至关重要。

携手共同应对挑战

加强合作的模式包括设立一个新的全球秘书处来管理开源，或建立一个开源软件社区领导人的对等网络。

Contents

前言

开源大会报告前言

在飞速发展的数字时代，开源作为人类集体知识库，成为了希望和进步的灯塔。开源的根基在于其透明性、包容性和社区驱动开发的核心原则；开源代表了一种超越边界和文化的协作。从2023年开源大会中汲取的洞察显示，开源的力量不仅仅在于其代码，更在于培育它的全球社区。

开源的韧性是我们共同努力的结果。在我们应对网络安全、人工智能以及技术民族主义兴起等复杂情况时，确保开源软件的安全显得尤其重要。安全是我们互联世界中至关重要的问题，零星的修复和补丁只能提供暂时和短期的解决方案。要从根本上解决开源安全问题，需要一套系统化和整体性的解决方案，不仅要解决安全漏洞的症状，更要解决其问题的本质。这是对开源基础设施服务提供商和从业者的紧迫呼吁，带头倡导“默认安全”的原则。易于获取的安全工具、健全的标准、协议和最佳实践能够赋予开发者从根本上加固他们产品的安全性。

开源软件日益广泛的应用使处于一个重要的十字路口，面临着日益严格的监管审查。随着监管审查的加剧，积极主动的政策倡导和教育工作显得尤其重要。没能得到足够反馈的监管可能会威胁到开源的根本价值。这种由于对开源本质缺乏理解而采取的措施，有可能扼杀创新、设立合作壁垒，并导致全球开源社区的分裂。拥有法律专业知识、沟通能力和社区参与度的开源基金会具有独特优势，可以在政策领域进行倡导，确保监管与开源原则兼容。

随着人工智能持续渗透到我们生活的方方面面，开源原则变得更加重要。开放和透明成为解决人工智能安全的核心要素。通过在人工智能开发中采用开源原则，人工智能系统将不仅强大，还将是道德、可追溯和安全的。

展望未来，多样性、包容性和共享规范将继续成为开源增长和影响的基石。无论是通过全球秘书处还是点对点网络，建立全球开源社区的统一战线模式将有助于确保开源仍然是人类的集体知识库。我们希望能够团结一致，共同应对我们所面临的挑战，塑造一个更加光明、更加开放的未来。

携手开源

陈岳，技术战略主管

Chris Xie，开源战略主管
Futurewei 科技有限公司

引言

自 20 世纪 80 年代以来，开源已从一场草根运动发展成为技术和社会创新的重要推动者。将软件源代码免费提供给任何人查看、修改和分发的理念全面改变了全球软件行业。但它也成为其他领域合作和创新的强大新模式。

到了世纪之交，对软件开发的共享方式催生了围绕开放标准、开放硬件和开放数据的大规模协作努力。[1] 因此，当今几乎没有一个数字工具或应用不包含开源代码，或其开发者没有深受开源方法的深刻影响。

在数字时代，透明度、包容性和社区驱动发展的原则将继续影响我们如何创新、分享知识和解决复杂问题。在技术和软件开发领域之外，开放式协作正在推动深刻的制度变革，包括开放式政府、开放式科学和开放式教育的兴起。开源软件的协作性、透明性和成本效益也使其成为全球应对气候变化和治疗顽疾等问题必不可少的工具。

开源社区面临前所未有的挑战时代

经过几十年的持续进展，如今开源社区正面临着前所未有的挑战。例如，虽然强大的开源方法可以引发突破性的进展，但它们也容易被不良分子利用。就像专有软件产品可能会受到恶意行为者的攻击一样，开源本身的开放性使其容易受到网络罪犯和其他行为者的攻击，他们在开源项目中引入漏洞和后门。复杂的开源软件供应链攻击正在增加，并已提醒开源软件社区迫切需要加强其网络安全姿态。[2]

与此同时，开源软件的普及也加强了监管审查。仅在过去两年中，美国 CISA 开源安全路线图[3] 和欧盟的产品责任指令和网络韧性法案（CRA）已经采取措施增加了产品安全责任，并要求更及时地披露和修补安全漏洞。

遗憾的是，其中一些本意良好的监管举措对开源社区独特的开发、商业化和许可证模式的影响缺乏深入的理解。因此，它们带来了重大的合规挑战。有人认为，新法规可能会破坏开源开发模型，这个模型孕育了Linux、Apache Web服务器、Mozilla Firefox等众多基础数字基础设施中开创性的作品。随着监管挑战不断增加，开源软件基金会被要求帮助开发者遵守新法规，并更早地积极参与制定数字领域的新立法。

开源因社区对开放性、协作和信息跨境自由流动的坚定承诺而蓬勃发展。在这方面，社区也面临着跨境合作的新障碍。全球贸易紧张局势、地缘政治冲突以及数字主权的强调已成为国际数字技术合作的真正障碍。例如，所谓技术民族主义兴起促使包括美国和中国在内的许多国家对半导体和其他关键技术实施严格出口管制。许多开源社区人士担心限制技术贸易可能会导致开源软件开发分裂成区域性飞地，阻碍了社区内促进包容性并培养更多样性人才库的努力。

最后，人工智能系统在软件开发中的加速部署也给开源软件社区带来了困难。AI 启用的代码生成器可以将自然语言提示转换为完全编码的函数，仅需几秒钟即可完成。软件行业和其他领域生产力潜力不容忽视。然而，由AI模型生成的代码所涉及到的来源不确定性可能会导致意外滥用专有或许可代码，从而引起潜在侵权问题以及与许可和网络安全相关的其他担忧。

更广泛地说，当今对人工智能的大规模投资有望带来快速进步，包括在医疗保健、交通运输、公共管理、金融和教育等领域具有开创性的应用。与此同时，人工智能日益增长的影响力也带来了新的风险和伦理考虑，涉及偏见、透明度、隐私、就业流失以及对人类长期威胁等问题。竞相部署和商业化新一代人工智能技术的公司主要坚持保密和专有开发模式。与此同时，开源社区正在努力证明真正开放的人工智能方法，为确保AI系统符合人类价值观，并维护人权并促进整个社会福祉提供了更好的路径。

2023 年日内瓦开源大会

今天，开源的影响是全球性的，而全球性的覆盖和影响也带来了深远的责任。监管、技术民族主义、人工智能和网络安全正在改变开源领域的格局，并催生了集体行动的必要性。许多开源社区利益相关者认识到，迫切需要加强开源软件项目和支持它们的基金会之间更大规模合作，以便使社区成员在这些共同挑战上团结一致。

开源软件基金会在生态系统中拥有不同的任务、支持者和角色。过去，不同的哲学取向和观点曾妨碍了合作。然而，考虑到共同面临的挑战，来自全球开源软件社区的领导者最近放下了这些差异，并建立了新联盟，以确保生态系统持续成功。

在 2023 年 7 月,代表 37 个组织的 53 位开源领袖聚集在瑞士日内瓦参加了开源大会。该大会的任务是确定共同价值观、建立关键利益相关者之间的联系,并制定一个计划来维持开源的活力、韧性和完整性。

选择日内瓦作为大会的举办地是有象征意义的。作为著名《日内瓦公约》的诞生地,日内瓦长期以来一直是一个中立的场所,各国在这里解决分歧、寻求共同点。主权国家领导人经常聚集在日内瓦制定指导国际关系的交战规则——这些努力基于对推进人类福祉的共同承诺。

在类似的精神下,参加大会的开源领袖被要求超越地区分歧、意识形态差异和当代地缘政治氛围。与会者普遍认为,开源是一种超越国界的集体利益,依赖于国际合作和有效的生态系统治理。开源领导者现在面临的挑战在于制定相互承诺和行动计划,以确保忠实于社区的基本原则:公开性、包容性和社区驱动发展。

更具体地说,日内瓦大会与会者的任务是实现以下目标:

- 探讨和讨论开源社区面临的关键挑战
- 探索增强基金会间合作的途径,包括维护共同价值观的机制和应对共同挑战的策略。
- 建立新的渠道,以进行后续讨论,并保持日内瓦达成的任何协议所需支持行动的势头。

2023年7月27日上午,大会与会者参加了一系列围绕开源社区面临的四个紧迫挑战组织的小组讨论。

- **解密开源安全:**讨论如何通过解决安全漏洞和维护关键的开源基础设施来促进对开源软件解决方案的信任和信心。
- **技术政策对去中心化组织的影响:**围绕建立协调应对措施的圆桌会议,以拥抱可能影响开源软件开发和部署的新兴监管举措。
- **保持全球、开放和包容的合作:**对于地缘政治上的障碍,如出口管制和数字主权倡议相关的数据、半导体和其他关键技术,进行了重要审视。
- **人工智能是否改变了一切:**对开源生态系统可能面临的风险进行审查,包括许可证违规、版权侵犯、人力资本和社会公益。

下午,会议焦点转向将关键利益相关者聚集在一起解决开源社区最紧迫的挑战。与会者探讨了各种增强协作的机制,包括成立一个新的全球性秘书处来管理开源社区和创建一个轻量级对等网络以协调开源软件基金会的努力。日内瓦的讨论结束时,形成了以下共识:定期召集开源软件基金会领导人并共同努力管理全球开源生态系统具有巨大价值。本报告剩余部分记录了2023年开源大会的议程,并突出了这个重要日子中关键讨论点和结论。

与会者广泛认识到,开源是一种超越国界的集体利益,并且依赖于国际合作和有效的生态系统治理。

解密开源安全

与其他软件类别一样,开源软件也不免于安全漏洞。代码中可能存在缺陷,一旦被发现,就会被恶意行为者利用。这些漏洞可能来自编码错误、缺乏更新或安全审查不足等原因。攻击者最近针对软件供应链进行了攻击,在广泛使用的开源库和组件中注入恶意代码。这些攻击可能会危及许多依赖于这些库的应用程序,从而触发潜在的灾难性故障和违规行为,给依赖开源软件的组织带来严重后果。

鉴于事关重大,今天的第一场专题讨论会汇聚了开源社区的领导者,讨论围绕开源软件安全的关键问题以及增强其复原力的策略,也就不足为奇了。保护关键开源基础设施的安全已成为开源软件生态系统合作的焦点。 与会者认为,当务之急是建立对开源软件的信任和信心,并支持关键开源基础设施的持续维护。 辩论的关键问题是如何最好地组织开源软件社区来实现这些目标。

开源安全需要一种与维护者社区合作的新模式

去中心化创新正在为支持数字经济而广泛应用的开源组件织就一幅非凡的织锦。 正如大会与会者所解释的那样,这些组件被嵌入到从电网、航运、运输到电子商务和金融等众多关键基础设施中,为全球商业提供了基础。 了解哪些组件使用最广泛,哪些组件最容易被利用,对于开源生态系统和更广泛的数字经济的持续健康发展至关重要。 正如一位与会者指出的那样,这样做对于为日常互联网用户提供安全的基础设施也是至关重要的。

日内瓦的开源领导人指出,维护目前使用的不同开源软件组件是一项复杂的挑战,需要采取透明和协调的方法,并从开源基础设施的主要受益者那里获得更多的资金和资源。 更具体地说,大会与会者指出了几个相互关联的挑战。

其中一项挑战是跟踪开源软件的扩散和监控潜在的漏洞。 在整个供应链的生产应用中,有成千上万的开源软件包,要准确了解哪些开源软件组件得到了最广泛的使用,是一项非同小可的任务。 当出现安全事故时,由于缺乏确保质量和维护的中央权力机构,组织协调披露潜在漏洞并分配纠正问题的责任就变得十分困难。 开源生态系统需要能够应用通用流程和统一的最佳实践。

第二个挑战是维护目前使用的大量关键开源软件组件。 大会与会者指出,在大多数情况下,没有官方资源分配,也很少有维护关键开源软件安全的正式要求或标准。 虽然 Linux 等知名度较高的项目拥有活跃的社区并经常受到关注,但其他项目却很少更新,也很少有人关注。

默认情况下的安全意味着在设计和开发应用软件时,从一开始就将安全作为首要考虑因素,并使安全成为默认状态,而不是事后才想到 。

几位与会者建议对维护者进行补偿,使其专注于安全问题,特别是那些可能缺乏时间和资源进行定期更新和维护的维护者。 补偿并不一定需要投入额外的资金。EleutherAI 等开源软件项目通过将重要贡献者的名字添加到主要代码库和学术研究论文的引用数据中,激励贡献和维护活动。

大会与会者还对开源安全基金会(OpenSSF)所做的努力表示欢迎,该基金会已于 2021 年成为一个获得资助的项目。开源安全基金会在协调公共部门、私营部门和社区之间确保开源软件安全的努力中发挥着至关重要的作用。 一个关键职能是将资源导向无支持或资源不足的领域。 鉴于这项任务的规模,大会与会者呼吁增加可持续的资金来源,从源头和规模上解决安全漏洞问题。

尽管存在这些挑战,但大会与会者还是敏锐地指出,开源软件在本质上并不比专有软件更不安全。 事实上,开源可以为安全提供优势,例如透明度(允许任何人审查代码)、发现漏洞时社区的快速反应,以及针对特定安全需求定制和加固软件的能力。

开源软件生态系统必须帮助建立人才库,以应对安全挑战

如前所述,许多开源项目在资金和人员等资源有限的情况下运行。人力的缺乏可能会影响项目进行安全审计、应对漏洞或提供及时支持的能力。然而,大会参与者指出了另一个相关的系统性挑战:整个行业范围内网络安全专业人才的稀缺。

网络攻击和数据泄露在所有数字化产品和服务中的蔓延,提高了人们对网络安全的重视程度。随着威胁变得更加复杂,对于具备防范这些威胁技能的专业人才的需求显著增长。此外,随着云计算、物联网和移动设备的发展,攻击面显著扩大,给系统和数据安全带来了新的挑战。网络安全是一个涵盖多种专业领域的广泛领域,包括网络安全、应用安全、渗透测试、事件响应和法规遵从。大型企业在日益竞争激烈的全球人才市场上难以找到专业对口的人才,这使得开源项目面临的挑战更加明显。

鉴于这些挑战,大会参与者提出了一系列问题供开源软件社区考虑。我们能为社区提供哪些工具和培训,以便在安全方面取得更快的进展?我们能否重新定义什么是安全专业人员?我们能否增加我们开发者基础的多样性,从而吸引新的人才加入生态系统?我们能为增加计算机科学课程中对网络安全的重视做出贡献?

解决网络安全人才短缺问题的潜在方案可能包括网络安全培训计划和认证课程、与学院和大学合作创建最新的网络安全课程,以及多元化、平等和包容(DEI)倡议,以帮助填补人才缺口。大会参与者一致认为,开源软件基金会应在这些优先事项上开展进一步的讨论和行动。

最后，大会参与者提出了一项相关意见，许多小型企业依赖开源软件，但在管理IT安全方面的内部资源有限。一位与会者估计，95% 的小型企业没有专人管理软件安全。由于缺乏管理 IT 安全的资源，小型企业特别依赖开源软件社区提供及时的支持

开源软件社区应将 “默认安全” 作为优先事项

在结束关于网络安全的讨论时，大会参与者谈到了开源软件社区需要朝着 “默认安全” 模式发展的必要性。“默认安全” 意味着从一开始就将安全性作为设计和开发软件应用程序的主要考虑因素，并将安全性作为默认状态，而不是计划外的补救措施。在日内瓦集会的开源安全领导人认为，关键步骤包括在软件设计阶段早期定义安全需求，在生产阶段进行定期的安全审查，以及在软件部署后自动化进行安全测试、打补丁和合规性审计。

大会参与者一致认为，采用默认安全模式并自动化安全测试和维护流程将显著降低开源软件应用程序中安全漏洞和脆弱性的可能性。这也将为开发者和维护人员在生态系统中的其他关键任务腾出时间。正如一位参与者所说：“我们越能创造默认安全，就越能专注于更高层次的问题。”

各种数字化产品和服务中的网络攻击和数据泄露的增多，使人们对网络安全的重要性有了更深的认识。

技术政策对非集中化组织的影响： 挑战与机遇

围绕网络安全的讨论强调了为什么良好的治理和政策参与对于开源软件生态系统的持续成功和韧性日益重要。然而，除了网络安全，还有许多其他互联网政策问题对开源解决方案的用户和开发者构成了重大的挑战和机遇。例如，在知识产权、隐私、产品责任和反垄断等关键问题上，人们普遍认为，开源社区在技术政策对话中没有发挥应有的影响力或主动性，导致出现了可能威胁开源模式的监管举措。与此同时，开源软件提供了解决我们时代许多关键政策挑战的解决方案。然而，开源社区在政策圈中缺乏能见度，这意味着该社区的社会经济贡献往往得不到重视。

随着开源领袖在日内瓦聚集，讨论自然转向了最近的监管行动对开源生态系统的影响、教育全球政策界了解开源软件独特特性和方法论的需求，以及开源软件基金会优先考虑增强合作和能力建设，以有效进行政策参与和倡导的必要性。

开源软件的日益普及使监管成为必然

开源软件已成为当今技术领域最基本、最普遍的元素。由于它支撑着各个领域的创新、促进开发者和组织之间的合作，以及使人们能够平等地访问强大的软件工具和解决方案，其影响力持续增长。据估计，开源组件驱动了70%到90%的现代软件解决方案，包括从网页开发和机器学习到云计算、数据科学和科学研究的各种应用。[4]

随着开源软件的日益普及，监管审查也越来越严格。例如，Linux操作系统在服务器和云计算市场的主导地位引起了关于竞争和反垄断问题的担忧。像欧洲的《通用数据保护条例》（GDPR）这样的数据隐私法规，使人们关注用于数据处理和存储的开源软件包是否符合数据保护法。在Log4Shell事件之后，监管机构正在调查企业是否对开源组件进行了适当的管理并解决了安全漏洞。更广泛地说，对网络安全和关键基础设施的担忧导致了对开源解决方案在国家和企业网络安全战略中作用进行评估。

大会参与者将欧洲描述为技术政策的重要 “战场”，指出欧盟通常是技术政策的先行者，而美国则倾向于采取观望态度。事实上，欧洲监管机构在保护数据隐私、促进竞争、确保网络安全以及应对新兴技术带来的社会经济挑战方面，比任何其他司法管辖区都行动更快。仅在过去五年中，欧洲就出台了《GDPR》以建立数据保护和隐私标准，《数字市场法案》以监管大型数字平台并防止反竞争行为，《数字服务法案》以打击非法内容并提

高在线服务的透明度,《人工智能法案》以管理人工智能的开发和使用。最近,欧盟提出了《网络韧性法案》(CRA),以加强对具有数字元素的产品的网络安全要求,并更新了适用于数字时代的《产品责任指令》。

对欧洲技术政策及监管机构的批评是,尽管开源软件在数字经济中扮演着关键角色,但开源软件组织在立法过程中代表性普遍不足。缺乏与政策界的接触反过来又导致对开源生态系统的独特需求和观点、其方法论以及开源软件解决方案的社会经济影响缺乏考虑。与会代表认为,像《网络韧性法案(CRA)》这样的法规默认采用专有软件开发模式,并未正确理解或考虑到开源软件的独特特性,包括其开发和许可模式。参会的欧洲开源软件领导者预测,《网络韧性法案》的文档、认证和责任规定可能会对开源软件 开发产生寒蝉效应。[5] 同时,一个考虑到开源软件开发和分发的独特动态的更具包容性的监管程序,可能会增强网络安全并有利于开源生态系统。

政策宣传和教育对开源生态系统的持续成功至关重要

大会参与者最大的担忧是,政策制定者可能不理解开源生态系统的运作方式,并有意无意间出台,有可能打破使社区取得成功的合作模式的法规和政策。一些基金会领导人指出,政策制定者并不一定是所有监管领域的资深专家,因此他们依赖于行业内部人士的专业知识。在某些情况下,对重大技术政策问题缺乏协调一致的开源响应,造成了空白,并最终使得领域被规模更大、资源更丰富的实体所主导。

通常情况下,开源软件基金会没有资源来运作全职的政府关系组织。尽管如此,开源基金会在主要政策问题上一直很活跃。一些基金会领导人回忆说,在Log4Shell安全事件之后,他们花了很多时间向政策制定者普及有关开源组件的知识,但他们也指出,这些工作只是浮于表面。许多人呼吁开源基金会在向政策界介绍开放标准和开源的好处方面加大投入。

大会参与者确定了几个围绕政策制定者需要教育的关键问题。例如,什么是开放标准?开源收入模型是如何工作的?开源软件如何影响软件市场中的竞争和选择?以及,围绕互联网安全、产品责任和知识产权(仅举几例)的政策如何影响开源代码的生产和分发模式?

聚集在日内瓦的开源领导者普遍支持与政策制定者和监管者建立友好互利的关系。但是,大会参与者也警告说,开源软件社区必须警惕标准的潜在武器化。一位参与者指出,标准长期以来一直被用作国家经济战略的一个要素,围绕技术优势领域调整的标准努力可以赋予国家竞争优势。因此,存在着这样一种风险,即一些行为者会将标准进程作为推进国家利益和技术领先目标的一种手段,而不是让开放标准的发展顺其自然。国家行为者可能会将开源软件武器化,以推进地缘政治议程,这一现实突出表明,社区成员需要联合起来,捍卫开源软件的中立性,并强调其作为全人类集体知识库的重要作用。

有效的政策工作需要专业技能和开源软件基金会之间更多的合作

在日内瓦的讨论中,一个反复出现的主题是,政策倡导与开源软件的开发工作大相径庭,需要专门的技能组合和与更多的社区合作。一些大会参与者指出,软件工程师与在欧洲委员会等监管机构工作的政策人员之间经常存在脱节。因此,开源软件基金会的责任在于获得参与政策讨论所需的技能和知识,包括对监管机构如何制定政策的细致理解。其他重要能力还包括法律敏锐性和对监管环境的熟悉程度,向非技术受众传达复杂技术概念的能力,以及宣传、公开演讲和社区参与方面的技能,以帮助提高对特定技术政策的认识并争取支持。

大会参与者一致认为,影响有利于开源生态系统的政策变革不仅需要长期致力于能力建设,还需要投资于与政策界建立关系。一些参与者认为,影响政策可能是一个漫长的过程,通常需要持之以恒,和实现长期政策目标的能力。许多出席日内瓦会议的开源基金会还指出,他们目前在政策工作方面资源不足。尽管一些开源基金会正在聘请专业游说人员,但也有人建议基金会可以从其成员公司那里获得额外支持,许多成员公司都有广泛且资金充足的政府关系运营。正如一位与会者所指出的," 我们在政策圈中看到了更高水平的参与,但我们需要更多的资源和更持续的努力来建立关系" 。

最后,开源基金会的领导者们一致认为,在政策方面开展更广泛的社区合作,对于社区成功影响政策议程至关重要。大家普遍都存在这样的情绪,开源基金会在软件开发的合作方面表现出色,但在政策和治理方面的合作却差强人意。许多人希望看到开源基金会联合提出围绕网络安全、人工智

能、隐私、知识产权和其他相关事宜的新的政策建议。大会参与者还一致认为，需要进行更多讨论，以建立各个政策团队之间的联系，增强社区的政策倡导能力，并建立跨基金会的在政策问题上合作的结构。正如一位参与者所说："我们需要更好地相互理解，包括我们的章程和成员关切以及我们影响政策的努力，这样作为基金会，我们才能够更好地协调我们的努力。"

开源基金会有责任获得参与政策讨论所需的技能和知识 。

保持合作的全球性、开放性和包容性：检视出口管制、数字主权和 DEI（多元、平等、共融）的影响

几十年来，开源软件开发方面不受约束的全球合作使为开源项目做出贡献的优秀开发人员队伍不断壮大。 2022 年，来自 200 多个国家的 8,300 多万开发人员为 GitHub 上的开源项目做出了贡献。值得注意的是，GitHub 全球约 74% 的用户居住在美国以外，其中亚洲、拉丁美洲和东欧的开发人员所占比例显著增加。 与此同时，一些突破性的开源软件创新来自日本（Ruby）、芬兰（Linux）和南非（Ubuntu）等地。

虽然开源在全球取得了前所未有的成功，但聚集在日内瓦的社区领袖们表示担心，全球贸易紧张局势、地缘政治冲突以及对数字主权的日益关注，对开放和包容性合作构成了真正的障碍。 例如，日益高涨的技术民族主义促使美国、中国和其他国家加强了对半导体、无人驾驶飞行器、全球定位系统以及各种军用电子和软件系统等关键技术的出口管制。 社区领袖们讨论了技术民族主义政策是否会将开源软件的发展分割成地区孤岛，并阻碍促进更大包容性和深化社区人才库的努力。

鉴于这些风险，与会者权衡了各种方案，以帮助维持知识和技术的跨境自由流动。 大会与会者还讨论了使开源项目领导者能够整合多元化参与者并成功颁布开源准则、道德和最佳实践的措施。

数字主权为开源带来机遇和挑战

数字主权是日内瓦辩论的一个关键议题，包括加强国家对数字技术和数据流的控制的举措将在多大程度上促进或阻碍开源运动。 数字主权是指一个国家在不受外国政府或公司不当影响的情况下，控制其境内数字技术、数据和信息流的能力。 它所包含的理念是，一个国家应有权以符合其自身价值观、利益和安全关切的方式，就其数字基础设施、政策和法规做出决策。

近年来，各国纷纷推出数字主权措施，其动机往往是对数据隐私、国家安全、经济增长的关切，以及减少对外国技术提供商依赖的愿望。 例如，俄罗斯和中国已出台法律，规定在其境内实现数据本地化，并投资建设自己的云基础设施，以便在其境内存储和管理数据。 与此同时，欧盟于 2018 年实施了开创性的 GDPR，以确保为其公民提供更好的数据保护和隐私保护。 GDPR 之后又出台了《数字市场法》、《数字服务法》和《欧洲芯片法》，再加上即将到来的《人工智能法》，一起构成了一套全面的数字主权倡议。 这些新法律的目的不仅是为了捍卫欧盟公民在数字空间中的权益，也是为了增强欧洲公司的竞争力，使其能够与美国的大型技术公司竞争。[6]

虽然数字主权旨在为各国提供对其数字环境的更多控制权，但它也可能导致各种挑战，如互联网的碎片化、跨境数据流的障碍、与国际规范的冲突，以及软件开发商和技术公司的监管合规负担加重。 聚集在日内瓦的社区领导人认为，数字主权往往与监管协调的目标相悖。 开源基金会深知，不同国家和文化在处理技术政策问题时总会存在差异。 然而，新法规的激增增加了合规成本，领导人指出，对于资源不足的开源软件基金会来说，跟上全球技术政策的发展具有挑战性。 正如一位与会者所说，" 在急于对整个软件行业进行监管的过程中，有可能产生对开源造成附带损害的风险" 。

从好的方面看，本次开源峰会的几位与会者认为，数字主权工作也可能使开源社区受益。 例如，为了追求数字主权，一些国家正在采用开源软件，以

减少对专有技术的依赖。 一位大会与会者举例说,如果不利用开源和开放标准,欧盟就无法实现更大的技术自主权,而开源和开放标准可以让欧盟用户避免被供应商锁定,并获得对其技术栈的更多控制权。 换句话说,欧洲人不一定非要拥有源代码才能提高其数字自主权,因为欧洲在建设和使用开源解决方案方面的领导力,同样地提供了强效良方。

技术民族主义政策正在造成开源社区的分裂和孤立

数字主权主要是指各国政府希望在管理数字基础设施、政策和法规方面提高自主权,使之符合本国的当务之急。 然而,大会与会者警告说,在某些情况下,对数字主权的追求正与地缘政治竞争纠缠在一起,并煽动了日益增长的不信任气氛,也就是一些分析家所说的技术民族主义。

新加坡国立大学的亚历克斯-卡普里 (Alex Capri) 将技术民族主义定义为 “一种重商主义行为,将国家安全、经济繁荣和社会稳定等问题,与一个国家的科技能力和企业联系在一起” [7]。 在这种新的技术民族主义浪潮中,世界各国纷纷限制关键创新成果的境外转让,认为这样做可以刺激国家经济增长,增强国内竞争优势。 卡普里举例说,” 对有形硬技术的出口管制稳步发展,随后是对数据访问和使用的限制,最近又有了新的管制措施, …” 。 这将阻碍人力资本的自由流动和发展” 。

技术民族主义远远超出了巩固国家自治的范畴,还包括采取更加强硬的措施,在被认为可能主宰 21 世纪的技术领域 (从机器人技术和人工智能到工业互联网和先进的电信网络) 称王称霸。 世界主要经济体之间争夺国家技术优势的竞争如此激烈,以至于生态系统的领导者担心,地缘政治紧张局势和由此产生的政策干预可能会减缓技术进步,破坏开源软件社区赖以生存的国际合作。[8]

几十年来,技术推动了互联互通和全球协作的发展,开源软件就是其中的一个光辉典范。 与会代表指出,在当今的环境中,全球合作已经变得充满了政治风险,包括曾经无害的关于在哪里举办开源会议的决定。在某些情况下,总部设在西方国家的公司不愿意参与有地缘政治竞争对手公司参与的国际开源项目,因为他们认为存在法律上的不确定性以及国内政策反弹的风险。 在其他情况下,国际冲突或制裁导致来自不同国家的贡献者被排除在开源社区之外。[9]

与会者就技术民族主义政策和倾向对开源生态系统中的参与和社区管理的动态的影响提出了几个关键问题。 例如 : 我们如何与 “实体清单” (由美国管理的外国个人和组织名单上的公司公开合作? 美国商务部限制向参与威胁美国国家安全或外交政策利益活动的组织出口某些敏感技术和部件) ? 对于来自不同国家、可能被怀疑不可信的开源贡献者,我们该如何处理安全政策? 作为基金会,在俄罗斯入侵乌克兰之后,当开源贡献者因民族血统而受到骚扰时,我们应该如何干预?

日内瓦开源会议的讨论未能解决因地缘政治紧张局势加剧而引发的一些棘手问题。 不过,大会与会者就几项当务之急达成了一致 :

1. 与会者一致认为,开源基金会必须反对按照地缘政治划分社区及其关键平台,并倡导保持知识、技术和协作的跨界自由流动。

2. 开源的领导者希望避免出现这样的情况 : 在决定谁参与开源社区、以什么条件参与、达到什么目的等问题上,政治因素开始主导原本属于技术层面的决策。

3. 大会与会者指出,政治中立的姿态和管理社区贡献的透明协定是确保开源项目运作过程中,地缘政治紧张局势不会影响他们与优秀开发者合作的方式和时间的关键。

4. 与会者普遍认为,举办年度开源大会将促进国际对话,并在代表世界不同地区的开源软件基金会之间分享最佳实践。

5. 开源领导者还一致认为,在与政治家/政客和监管者接触时,开源软件基金会应宣扬 “在国界上封闭合作的国家将不如那些接受全球合作及其益处的国家成功” 的信息。

在当今环境下,全球合作已经充满了政治危险,包括关于开源会议地点的无害决定。

多样性和包容性是有关开放式协作的格局和对话的重要组成部分

开源社区曾经牢牢扎根于美国和西欧，如今却日益全球化和世界化。 例如，中国是开源技术的重要消费国和贡献国。 不仅近 90% 的中国公司使用开源技术，而且中国用户也是 GitHub 上仅次于美国用户的第二大高产群体。[10] 然而，中国并非孤军奋战。 许多新兴经济体都拥有庞大的开源开发者社区，包括印度、俄罗斯、韩国和乌克兰。 对于中低收入国家来说，与开源社区的接触正在催生新的创业企业，加快经济发展的步伐。

虽然开源在全球范围内蓬勃发展，但聚集在日内瓦的开源领导者们警告说，语言、文化和以西方为中心的传统体制对他们最大限度地发挥优秀开发人员的参与能力构成了障碍。 尽管开源社区日益国际化，但几位大会与会者认为，总部设在美国的组织在大多数开源项目的形成过程中具有超乎寻常的影响力。 反过来，北美参与者的霸权地位又会使发源于世界其他地区的开源项目黯然失色。

与会者担心，如果不能解决多样性和包容性问题，就会限制全球开源软件生态系统对人才和智慧的利用，从而削弱其最大限度地实现创新、取用和社会影响的能力。 一位与会者解释道：" 那些感觉不受欢迎的人将以其他方式建立技术。 不幸的是，这可能意味着最优秀的人才将建立专有技术，因为他们没有时间和资源来自由参与贡献。"

将不同语言和文化融入开源社区的挑战并非新问题，人们对目前的生态系统促进全球包容的能力充满信心。 不过，大会与会者认为，社会各界在促进全球包容方面可以做得更多。 例如，一些与会者强调有必要投资于项目交流的快速机器翻译能力。 虽然英语可能是软件世界的通用语言，但开源软件的领导者们坚持认为，项目交流的本地化可以推动北美以外的开发人员更广泛地参与进来。

大会与会者还讨论了促进开源规范、驯服行业中的大男子主义 "兄弟 " 文化以及在社区对话和决策中培养专业精神的重要性。 几位与会者指出，行为守则是建立社区规范、促进多元化参与和创造包容性环境的重要工具。 然而，行为准则在开源社区中常常引起争议，因为众所周知，开源社区对其自由和自治有着强烈的保护意识。 贡献者群体时不时的反弹使得社区规范和行为标准的执行成为一种微妙的平衡行为。 一些基金会工作人员报告说，他们曾因执行行为守则而受到骚扰。 日内瓦的与会者普遍认为，开源软件基金会应共同努力，以协调的方式制定和执行行为守则，促进社区的多样性和包容性。

人工智能会改变一切吗？ 什么是开放？ 责任、道德、价值观。

人工智能可定义为计算机执行以前需要人类智能才能完成的任务的能力，如感知、学习、推理、解决复杂问题和决策。 它是一个广泛的领域，包括机器学习、自然语言处理、计算机视觉、机器人学和专家系统等多种技术和方法。

近年来，人工智能日益融入我们的日常生活。 人工智能驱动的应用和服务，如生成式人工智能、语音助手、推荐系统和个性化广告，甚至是个性化广告牌，已经变得司空见惯。 然而，数字体验的转变仅仅是个开始。 从机器人手术到自动驾驶汽车，从革命性的生物技术研究到读取 CT 扫描结果，越来越多的智能机器将应用于医疗保健、法律和金融服务、交通运输、建筑、农业、制造业等领域。

如今，谷歌、Meta (Facebook)、微软、IBM、腾讯、阿里巴巴、AWS 等公司，以及大多数拥有海量数据集和计算能力的大型企业推出了大量人工智能计划。 国际数据公司 (IDC) 预测，在可预见的未来，人工智能支出的复合增长率将达到 26%。 这种滚雪球式的投资将持续十年，使投资额增长 10 倍以上。 不仅仅是软件公司。 2023 年中期，摩根大通 (JPMorgan) 约有 40% 空缺职位与人工智能有关，包括数据工程师和定量分析员，以及道德和治理职位。

对于开源软件社区来说，人工智能带来了一系列机遇和挑战。 聚集在日内瓦的社区领袖们讨论了对齐人工智能开源定义的必要性，以及人工智能代

码生成器在许可协议、安全和知识产权方面带来的挑战。 最后,大会与会者还思考了人工智能对社会的广泛影响,以及开源社区在解决偏见、隐私和人类生存威胁等问题方面的作用。

人工智能的开放性不仅仅意味着可以访问源代码

在关于负责任地发展人工智能的讨论中,关于人工智能开放性的性质和意义的讨论是一个焦点。 大会与会者就一系列相关问题展开了争论。 我们对负责任的人工智能有何期待? 能获取源代码就能算作开放吗? 对于人工智能模型和工具的开发者来说,什么程度的透明度才是合理的?

对于开源软件来说,开放性的定义是公认的。 根据 OSI 的开源定义,开源软件是带有源代码的软件,任何人都可以检查、改进和分发。[11] 此外,在开源软件的使用、修改和分发方面,有一些框架、许可证和法律理解来规范开发者和用户的权利。

同样的开源软件协定和定义无法无缝移植到人工智能系统中。 正如 Stefano Maffulli 在最近的一篇博文中写道:" 当你发现 [开源软件代码中的] 错误时,你知道该怪谁,知道该向哪里报告,也知道该如何修复。 但说到人工智能,你是否也有同样的理解,知道需要做什么才能修复漏洞、错误或偏差?[12] Maffulli 和日内瓦的许多大会与会者都明确表示,答案是否定的。

人工智能领域主要致力于创建能够处理和分析数据、学习模式并根据编程规则和统计模型做出决策的系统,或者仅仅从数据本身得出联想和想法的系统。 由于神经网络的决策过程是基于数以万亿计的数据点推断出的统计概率,因此超出了人类的理解范围,其基础模型被称为黑盒子。 仅仅研究人工智能的源代码并不一定能解释或揭示人工智能系统产生输出结果的原因。 就连人工智能开发人员也承认,他们无法轻易解释他们正在开发的人工智能系统的产出。[13]

日内瓦大会的与会者认为,提高可解释性意味着提高表达人工智能系统为何做出特定决定、建议或预测的能力。 可解释性之所以重要,是因为它提高了系统的可信度、安全性和责任感,而这些系统越来越多地影响着诸如疾病诊断或决定谁能获得信贷等改变生活的决定。 正如路易斯维尔大学计算机科学教授 Roman V. Yampolskiy 在最近的一篇论文中解释的那样:" 如果我们拥有的只是一个' 黑盒子',就不可能了解故障原因并提高系统安全性"。 Yampolskiy 接着说,在没有解释的情况下相信人工智能的答案,就等于把人工智能当成神谕系统。 Yampolskiy 说,危险在于 " 我们无法判断 (人工智能系统) 是否开始提供错误或操纵性的答案"。[14]

大会与会者表示,开发人工智能可解释性的能力需要了解模型架构,包括模型中不同变量的权重以及用于训练模型的数据类型。 遗憾的是,人工智能系统越是复杂,就越难准确地指出它是如何获得特定洞察力的。 事实上,一些人工智能专家声称,人工智能的性能与可解释性之间存在权衡。[15] 换句话说,让人工智能模型具有可解释性可能会降低它们的有效性,因为这样做意味着需要降低模型的复杂性 (例如,使用决策树或线性回归而不是深度神经网络),并在更小、更集中的数据集上训练模型。

让人工智能更加透明的另一个干扰因素是人工智能系统的运行规模。 正如 Maffulli 所说:" 人工智能消耗和产生的数据量以 TB 和 PB 为单位,这意味着需要特殊的硬件才能对如此规模的数据集进行快速计算...。 不幸的是,建立和运行这些大型人工智能模型所需的硬件是专有的,价格昂贵,而且需要特殊的知识来设置"。[16] 简而言之,运行这些模型所需的巨大计算能力使得第三方组织很难对输出结果进行质问。 因此,让谷歌、Meta 等公司将其模型和系统提交外部审计和可靠性测试,可能凸显人工智能的局限性和偏见问题的部分解答。

人工智能生成的代码将在开源许可、安全和监管方面带来挑战

日内瓦会议的另一个讨论重点是人工智能驱动的代码生成器在软件开发领域的日益凸显。 在过去几年里,GitHub 的 Copilot 和 OpenAI 的 Codex 等新工具让开发人员惊叹不已,它们不仅能生成简单的代码行,还能根据自然语言提示生成完整的编码功能。 以前可能需要数小时甚至数天的编码任务,现在只需几秒钟就能完成。 GitHub 估计,到 2030 年,人工智能编码将使全球 GDP 增长 1.5 万亿美元。[17]

与其他大型语言模型一样,人工智能代码生成器也是在海量数据集 (包括 GitHub 和其他平台上托管的大量开源代码库) 上训练出来的。 好的一面是,开源库包含了全球开发人员编写的大量不同代码。 这些资源库涵盖了大量编程语言、范式和应用领域,为训练人工智能模型提供了丰富而

详尽的真实世界代码。 从本质上讲,它们反映了全球开发者社区的经验和集体智慧。

正如大会与会者所指出的,不利之处在于,人工智能代码生成器的使用越来越多,这带来了一系列与许可、安全和监管合规有关的挑战。 这些挑战源于人工智能模型生成的代码缺乏出处。 例如,OpenAI 的 Codex 并不包括其生成的代码片段所依据的原始代码的许可方案信息。 因此,要确定生成的代码是专有代码、开源,还是属于其他许可计划,可能会很困难。这种不透明性造成了无意中滥用专有或授权代码的风险,从而导致潜在的侵权问题。 对于人工智能代码生成器是否会重现其所训练的代码库中存在的错误和安全漏洞,人们也提出了类似的担忧。[18]

使用人工智能生成的代码还引发了这样的问题:它们生成的新软件应用程序是否应受开源许可的约束,因为人工智能代码生成器已经在大量开源的基础上进行了训练。[19] 换句话说,人工智能生成的代码是否应被视为开源代码库的 “衍生作品”?

日内瓦的讨论最终没有解决这些难题。 不过,与会者一致认为,开源软件基金会应合作制定新的框架,用于处理人工智能生成的代码,因为人工智能很可能是未来软件开发中无处不在的工具。

人工智能带来的系统性风险需要紧急的开源应对措施

对人工智能开发的大量投资有望带来快速进步,使人工智能系统能够应对日益复杂的挑战,并对人类生活的各个方面产生积极影响。与此同时,大会与会者警告说,人工智能日益增长的影响力引发了与偏见、透明度、隐私、工作取代和对人类生存威胁相关的新风险和道德考虑。

以偏见和歧视为例。人工智能系统可以继承或放大它们所训练的数据中存在的偏见。如果训练数据包含偏见或歧视模式,人工智能系统可能会强化甚至加剧这些偏见,导致招聘、贷款或刑事司法等领域出现不公平的结果。例如,根据历史贷款数据训练的人工智能系统可能会延续歧视性贷款做法,导致边缘群体获得信贷或贷款的机会不平等。使用人工智能算法来识别犯罪热点并分配警察资源的预测警务系统因过度针对少数族裔社区而受到批评。

人工智能引发的歧视可能很难被发现,甚至更难被抵制,因为偏见本质上已经融入到训练模型的数据中。如上所述,目前人工智能模型如何运作缺乏透明度,使得人们无法理解人工智能系统如何得出结论或预测。当决策逻辑和大量底层数据几乎无法拆解或逆向工程时,如何识别和解决任何潜在偏差?

偏见和歧视在大多数情况下是训练人工智能的意外后果,这是因为训练数据反映了社会偏见和权力结构。然而,像人工智能这样强大的技术不可避免地会导致其能力被恶意利用。事实上,AI、算法和自动化事件(AIAAIC)争议库表明这种滥用已经司空见惯。该组织(AIAAIC)的最新报告发现,2021 年新报告的人工智能事件和争议数量是 2012 年的 26 倍。作者得出结论称:“报告事件的增加很可能是人工智能越来越深入现实世界和人们对人工智能道德滥用方式的认识不断增强的证据。[20] 2022 年的著名事件包括乌克兰总统弗拉基米尔·泽连斯基 (Volodymyr Zelenskyy) 呼吁其军队放弃对俄罗斯的战斗的深度伪造视频,以及 “机器人” 在选举、新闻议题和社交媒体上的使用前所未有地增加。非常有可能的近期风险还包括恶意行为者可能会控制网络物理系统,以破坏性的方式使用它们,例如勒索关键基础设施、使自动驾驶车队崩溃,或将商用无人机变成面部定位导弹。[21]

偏见、欺骗、工作流失以及人工智能助长的犯罪和恐怖主义成为了日益加长的风险名单里的头号风险。然而,最终的存亡危机问题可能是,既然人工智能的精灵已经从魔瓶里出来了,人类是否还能控制人工智能。大多数人工智能专家预测,人工智能系统最终将达到超级智能的水平——表现出超越人类的智能。超级智能的潜在时间表是一个引起大量猜测和争论的话题。然而,一旦发生这种情况,人工智能系统可能会优先考虑自己的目标,并以对人类有害的方式行事。

考虑到现在的状况,日内瓦的开源软件领导人对为更好地理解挑战并确保负责任地开发和部署人工智能技术而正在进行的各种努力表示欢迎。最值得注意的是,2023 年 3 月 29 日,超过 5000 名人工智能社区成员签署了一封公开信,呼吁暂停 GPT-4 等大型语言模型的进一步开发至少六个月,直到风险得到适当研究和缓解。 。著名的签名者包括 OpenAI 联合创始人埃隆·马斯克 (Elon Musk); Emad Mostaque,伦敦 Stability AI 创始人;和苹果联合创始人 Steve Wozniak,以及来自 Amazon、DeepMind、Google、Meta、Microsoft 等公司的工程

师。[22] 公开信呼吁建立“新的、有能力的监管机构”、“强大的审计和认证生态系统”以及“资源充足的机构来应对人工智能可能造成的巨大经济和政治混乱”。他们补充道：“只有当我们确信强大的人工智能系统会产生积极的影响并且风险可控时，才应该开发强大的人工智能系统。”[23]

这封公开信象征着人工智能界的关注程度。然而，拟议的暂停措施引发的问题和它回答的问题一样多，包括暂停措施是否可以强制执行。事实上，在这个即将成为数万亿美元产业的竞争中，任何政府或公司似乎都不太可能单方面迫使其人工智能技术领导者暂停开发，并冒着将重大优势拱手让给竞争对手的风险。[24]

在医疗、交通、公共管理、金融、教育、娱乐等领域的突破性应用将带来显着的社会和经济效益，但也带来相当大的风险。随着公司竞相部署新一代人工智能技术并实现赚钱盈利，参与人工智能开发的所有利益相关者应谨慎地致力于人工智能开发的道德准则或原则。

对于聚集在日内瓦的开源软件领导人来说，负责任地开发和部署人工智能的关键不一定是暂停，而是致力于提高其开放性和透明度。尽管许多最大的人工智能系统开发商都主张保持其人工智能模型的封闭性，但多位日内瓦大会与会者认为，公开开发人工智能模型具有优势。这些优势包括增加代码关注的数量以及创建确保人工智能系统值得信赖所需的透明度。

简而言之，日内瓦讨论中形成的共识是，人工智能的开放性为解决人工智能的弱点和挑战提供了更好的途径。一些人认为，科技公司正在非常迅速地推动系统部署，然后声称他们将在发现偏见和其他问题时处理这些问题。开源领导者坚持认为人工智能社区应该致力于更高标准的负责任开发。负责任的开发包括在不同的数据集上训练人工智能系统，并从一开始就将道德、安全和算法透明度融入到人工智能模型中，而不是事后才想到。其他措施可能包括数据收集指南、严格的测试协议以及减少偏见和歧视的审计实践。正如一位与会者所说，“人工智能开发人员无法解释大型语言模型输出的观点已不再被接受。我们需要突破技术界限，使输出透明且可解释。”

随着底层技术的成熟，人工智能将执行越来越多当今需要人类智能的任务，例如学习、推理、解决问题、感知和决策。在医疗保健、交通运输、公共管理、金融、教育和娱乐等领域的开创性应用将带来显著的社会和经济效益，但也存在相当大的风险。随着公司竞相部署和商业化新一代人工智能技术，所有参与人工智能开发的利益相关者，应慎重地承诺遵守人工智能开发的道德准则或原则，以促进透明度、问责制、公平性和负责任地使用人工智能技术，确保人工智能系统符合人类价值观和社会福祉。最重要的是，对开源方法的承诺将确保人工智能的部署方式符合人类价值观、保障人权并促进社会的整体福祉。

开源协作的必要性

日内瓦开源领袖之间的晨间讨论深入探讨了开源生态系统面临的几个关键挑战。一位与会者生动地将这些挑战描述为开源协作面临的四大威胁：网络安全和关键基础设施的韧性；威胁开源模式的新兴监管举措；日益增长的技术民族主义以及促进开源项目多元化参与的需要；以及人工智能对开源许可、安全和知识产权的影响。

这些领域的一个首要主题是需要加强开源软件基金会和全球开源生态系统中其他主要利益相关者之间的合作。下午的焦点转向如何将主要利益相关者聚集在一起，应对开源社区面临的紧迫挑战。

确定开源生态系统的共同优先事项

在讨论潜在的合作机制之前，大会与会者回顾了需要加强合作的核心问题。

- **确保开源基础设施的安全。**大会参与者希望开源软件基金会能够合作，完善开源生态系统管理网络安全问题的方法。关键优先事项包括投入更多资源来维护关键的开源软件基础设施、建立更深层次的网络安全专业人员人才库，以及转向具有增强的自动化测试、修补和审核功能的默认安全模型。正如一位与会者所说，“如果我们不解决这个问题，我们将看到越来越多的监管审查。”

- **加强政策协作以维护开源开发模式。**随着监管审查的加强，开源领导者呼吁开源软件基金会在政策参与方面采取积极主动的立场，并更早地参与政策审议过程。大会与会者敦促开源软件基金会招募经验丰富的政策战略家，并在关键问题上加强协调。 “我们需要通过合作应对威胁，”一位与会者表示。 “开源背后的一支更强大的军队将有助于推进我们的价值观和当务之急。”

- **扩大政策参与。**开源领导者还希望看到开源软件基金会能够更加包容那些在许多政策合作中基本上被排除在外的大型支持者。与会者指出，美国和欧洲的组织之间存在许多政策合作，而中国、印度和巴西等国家的贡献者数量巨大，但参与政策制定的程度却很少。一位与会者表示：“我们必须在各国之间架起桥梁，让其他声音参与对话。”

- **防止区域碎片化。**大会与会者在很大程度上同情各国为加强数字主权所做的努力。一些人认为开源软件在使各国能够更好地控制其数据和数字基础设施方面发挥着实质性作用。然而，开源领导者担心全球贸易紧张局势和地缘政治冲突对开放和包容性合作构成真正的障碍，并希望开源软件基金会共同努力，避免开源项目的区域分裂和孤岛。

- **通过调整开源社区的行为准则来促进包容性。**大会与会者建议，协调整个社区的行为准则语言有助于为开源软件项目创建共同的期望和规范。其他人则呼吁外部仲裁支持，例如召集中立同行社区来帮助裁决行为准则问题。虽然也有人支持开源软件基金会的通用行为准则模板，但一些与会者指出，任何模板都必须足够灵活，以适应区域和文化差异。[25]

- 管理人工智能的机遇和挑战。与许多其他领域一样，人工智能正在给软件开发带来彻底的变化。大会与会者一致认为，开源软件社区需要一种集体的方法来应对人工智能，因为它改变了开发人员生成开源代码的方式。合作领域包括创建用于训练大型语言模型的数据共享以及检查人工智能对许可证和知识产权的影响。大会参与者还希望就社区如何定义开放人工智能达成一致，许多人认为这是管理日益强大的人工智能系统所带来的社会经济风险和挑战的更好途径。

虽然将集体注意力集中在对开源模式的威胁上是自然且至关重要的，但大会与会者还认为有必要更加公开地宣传开源社区所产生的公共利益，从互联网的基本支撑到强大的软件解决方案的广泛应用，涵盖了从经营企业到应对人类最紧迫挑战的各个方面。大会与会者敦促开源软件基金会联合起来，保护和增强世界各地的开发人员花费无数时间构建的技术共享。正如一位参会者所说：“作为一个社区，我们的目标不仅仅是具有成本效益的软件，我们正在实现对软件和计算的控制。我们的定位和影响力需要全球化。”

创建有效协作的结构和流程

在确定了全球开源社区的一系列共同优先事项后，大会与会者将注意力集中在促进协作的机制上。在研究这些选项时，开源领导者提出了两种潜在的协作模型。

- 全球开源秘书处。几位大会与会者提出了建立一个新的全球秘书处的理由，或者一些人所说的开源社区的联合国。新全球实体的倡导者指出，大多数行业都有国际协会，这些协会生产集体商品并代表其成员进行游说。另一方面，开源社区拥有大量且多样化的区域性、基于部门和基于项目的基金会，以满足其独特成员的需求。然而，开源生态体系缺乏总体结构或组织来促进社区的共同利益。一位与会者表示，当今跨基金会间合作的临时方法是随意的，使开源社区在监管和政策方面的处理显得不专业和无组织。

  大会与会者讨论了是否有可能让现有组织代表社区承担全球管理职责。正如一些人指出的那样，已建立的开源软件基金会拥有明确的任务和资源，可以根据其成员组织确定的优先事项来实现目标。因此，它们不一定具备能力或资金来为整个生态系统发挥更大的全球协调和倡导作用。然而，一些与会者指出，开放源代码促进会（Open Source Initiative: OSI）已经通过其开放政策联盟（Open Policy Alliance）与合作伙伴联盟合作，为与开源软件、内容、研究和教育相关的公共政策决策提供信息。[26] 正如一位与会者所解释的那样，“我们需要真正具有全球性和代表性的东西。如果秘书处拥有资源、深厚的政策专业知识、中立的定位以及为整个生态系统服务的使命，那就太好了。”

支持新的全球秘书处的发言者对现有开源软件基金会应对集体、整个生态系统挑战的带宽有限表示担忧。尽管大家都表达了需要深化整个生态系统合作的良好意愿，但一些人担心基金会间的合作可能会因履行现有任务的日常工作而被搁置。一般来说，开源软件基金会之间的合作资金是有限的。正如一位参与者所说，“如果这不是某人的工作，它就无法完成。”

- 用于协作的轻量级点对点网络。争论的另一方则认为，开源软件基金会执行董事所组成的网络（或者在某些情况下，政策领导的同行小组）足以满足生态系统的许多关键需求。支持轻量级生态系统协作方法的大会与会者对建立需要对人员和基础设施进行大量投资的新全球实体的好处持怀疑态度。他们指出，生态系统中已经存在多个**超组织（Meta-Organization）**。此外，他们相信现有开源软件基金会领导人有能力定期聚在一起，确定共同的优先事项，并分配管理协作工作的责任。

日内瓦讨论的结论清楚地表明，需要进一步对话来确定构建全生态系统合作的最佳路径。不管机制如何，继续在日内瓦开始的对话得到了广泛支持。大会与会者表示，从短期来看，保持势头至关重要。一些人建议，一系列配备简单协作工具的跨基金会间的工作组可以在网络安全、监管和开放人工智能等问题上取得进展。”

举办一年一度的开源大会也得到了大力支持，与会者普遍认为，他们认为定期召集开源软件基金会和其他利益相关者的领导人具有巨大的价值。正如一位与会者所说，“今天，我们的组织是支离破碎的，但当我们团结起来时，我们可以变得更加强大。”

展望未来，人们一致认为，加大开源治理的包容性至关重要。来自欧洲和北美以外的参与者观察到，当今的许多开源聚会都是以西方为中心的。他们希望看到包括实时翻译在内的包容性流程。人们还广泛支持在世界上传统上代表性不足的地区轮流举办一年一度的开源大会。

大会与会者还希望现有开源软件基金会社区为新兴基金会提供更多支持。例如，在亚洲、非洲和拉丁美洲，有广泛的开发者社区和许多临时用户组，但正式的基金会很少。为了促进更多地参与治理和政策参与，可能需要更多以区域为重点的基金会来代表这些区域。一些与会者建议，新基金会的导入流程可以帮助将知识从成熟的基金会转移到新兴的开源软件组织。同行网络和基金会索引也将帮助新的基金会领导者感受到与生态系统的联系更加紧密。

总结

最后，大会与会者一致认为，在日内瓦聚会所投入的时间和资源是值得的。来自世界各地的开源领导者有机会在亲密的环境中会面，许多人是第一次互相认识。主题专家在小组讨论中讨论了关键问题。确定并讨论了共同的优先事项。会议提出并讨论了深化全生态系统合作的可能方案。最重要的是，与会者坚定了继续对话并深化未来合作的决心。

当然，空谈不如实证。现在，生态系统的领导者必须团结起来，支持合作并继续开源社区的重要工作。不断上升的技术民族主义、新法规和新的网络安全威胁将带来挑战。一个更加团结和协作的开源社区将更成功地解决这些问题。聚集在日内瓦的开源软件基金会领导人致力于引领这一潮流，并且肯定会有更多人加入他们的行列。正如一位与会者恰当地宣称的那样："我们在这里所做的合作是为了支持数十万开发人员，他们正在开发价值亿万美元的软件，并在此过程中改变世界。"

鸣谢

作者要感谢聚集在日内瓦的 53 位开源社区领袖的贡献，他们的见解和评论为本报告提供了灵感。我要感谢 Futurewei 的 Chris Xie，他的领导和贡献使开源大会得以召开，并感谢 Linux 基金会团队主办了一场鼓舞人心的活动并发布了这份报告。热烈感谢 Jerry Michalski 的团队合作，为大会奠定了知识基础，并激发了日内瓦的社区对话。我还要特别感谢那些花时间审阅早期草稿并提供宝贵建议和见解的人，包括 Omkhar Arasaratnam、Stella Biderman、 Mirko Boehm、Jory Burson、Thierry Carrez、Stefano Maffulli、Mike Milinkovich、Deb Nicholson 和 Rebecca Rumbul。

关于作者

安东尼是 DEEP 中心的创始人兼总裁，也是商业和社会数字革命、创新和创造力方面国际公认的权威。他（与 Don Tapscott）合著了开创性的畅销书《维基经济学》及其后续著作《宏观维基经济学：互联星球的新解决方案》。

除其他任命外，安东尼还担任**区块链研究所**的研究主任、**马克尔基金会**美国经济未来倡议的专家顾问以及布鲁塞尔**里斯本理事会**的高级研究员。安东尼最近担任美国国家研究委员会**美国环保局未来科学委员会**的委员、**多伦多大学蒙克全球事务学院**的客座研究员以及巴西免费教育项目的首席顾问。他在技术和创新方面的工作曾在《哈佛商业评论》、《赫芬顿邮报》和《环球邮报》等出版物上发表过专题报道。

参考

1 https://academic.oup.com/book/44727/chapter/378967711

2 https://linuxfoundation.eu/newsroom/the-rising-threat-of-software-supply-chain-attacks-managing-dependencies-of-open-source-projects

3 https://www.cisa.gov/resources-tools/resources/cisa-open-source-software-security-roadmap

4 https://www.linuxfoundation.org/blog/blog/a-summary-of-census-ii-open-source-software-application-libraries-the-world-depends-on#:~:text=Introduction,and%20non%2Dtech%20companies%20alike

5 https://newsroom.eclipse.org/news/announcements/open-letter-european-commission-cyber-resilience-act

6 https://www.brookings.edu/articles/the-geopolitics-of-ai-and-the-rise-of-digital-sovereignty/

7 https://thediplomat.com/2020/09/us-china-techno-nationalism-and-the-decoupling-of-innovation/

8 https://www.channelnewsasia.com/business/risc-v-group-says-restrictions-open-technology-would-slow-innovatio N-3833631

9 https://www.computer.org/publications/tech-news/community-voices/on-the-weaponization-of-open-source

10 https://merics.org/en/short-analysis/china-bets-open-source-technologies-boost-domestic-innovation

11 https://opensource.com/resources/what-open-source

12 https://opensource.com/article/22/10/defining-open-source-ai

13 https://www.vice.com/en/article/y3pezm/scientists-increasingly-cant-explain-how-ai-works

14 https://philarchive.org/archive/YAMUAI

15 https://www.linkedin.com/pulse/interpretability-vs-performance-trade-off-balancing-model-shirsat

16 https://opensource.com/article/22/10/defining-open-source-ai

17 https://www.wired.com/story/fast-forward-power-danger-ai-generated-code/

18 https://www.wired.com/story/fast-forward-power-danger-ai-generated-code/

19 https://www.lexology.com/library/detail.aspx?g=4d3d8be3-abeb-430b-a7ab-bae434d3e014

20 https://aiindex.stanford.edu/report/

21 https://www.cam.ac.uk/Malicious-AI-Report

22 https://www.theguardian.com/technology/2023/mar/29/elon-musk-joins-call-for-pause-in-creation-of-giant-ai-digital-minds

23 https://www.bloomberg.com/opinion/articles/2023-04-05/an-ai-pause-would-be-a-disaster-for-innovation

24 https://www.brookings.edu/blog/techtank/2023/04/11/the-problems-with-a-moratorium-on-training-large-ai-systems/

25 OpenSSF: https://openssf.org/community/code-of-conduct/
CC: https://opensource.creativecommons.org/community/code-of-conduct/
Meta: https://opensource.fb.com/code-of-conduct/
Amazon:https://aws.github.io/code-of-conduct

26 https://opensource.org/programs/open-policy-alliance/

THE LINUX FOUNDATION | Research

Linux 基金会研究中心成立于 2021 年，致力于探索不断扩大的开源协作规模，提供对新兴技术趋势、最佳实践和开源项目的全球影响的见解。通过利用项目数据库和网络，并致力于定量和定性方法的最佳实践，Linux 基金会研究中心正在创建开源见解的首选库，以造福世界各地的组织。

要引用这项工作，请引用如下内容：Anthony Williams，“携手应对共同挑战：2023 年开源大会报告”，Yue Chen和 Chris Xie 的前言，Linux 基金会，2023 年 12 月。

本文的翻译由开源社国际组翻译及审校

组织：李思颖 Mabel

翻译： 刘天栋 Ted, 庄表伟, 陈超群, 李思颖 Mabel, 李明康, 瞿杰 Tony

审校： 刘天栋 Ted, 刘文涛 Leo