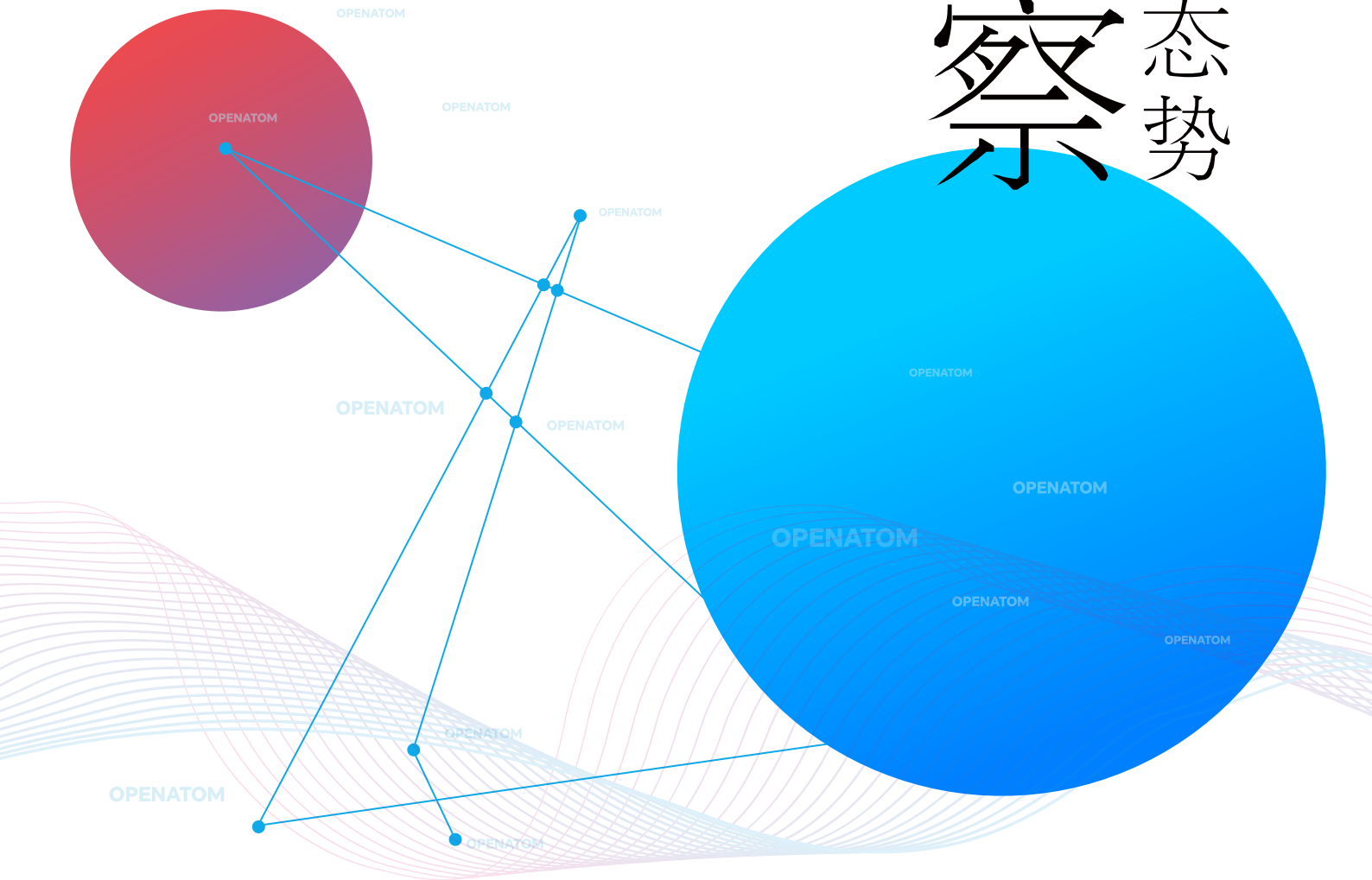
开放原子开源基金会
OPENATOM FOUNDATION

更好的开源
大家的洞察

2023·11

Insight
OPENATOM

洞察开源态势



PREAMBLE

卷首语

时间回到今年夏天，彼时，开放原子开源基金会正好走过了三个年头。《开源态势洞察》也正好出了十二期。基金会的行研团队也迎来了更多的同事，既有经验丰富的开源布道者，也有充满活力的年轻人，这群充满激情的同事们开始策划洞察的全新改版。

策划里面有一段话是这样描述的：“当前的开源领域，蕴藏着众多专业的实践经验，希望《开源态势洞察》能搭建一个平台，一端连接开源实践专家，另一端连接着积极参与开源或是对开源实践抱有疑问的组织及个人。洞察的目标是要将行之有效的见解或是方法论送到真正有需求的人的手上，期望成为业内人士获取洞见及灵感的宝贵资源。”开放原子致力于“繁荣开源事业，共享开源价值”，深知推广开源文化，普及开源实践的重要性。作为开源领域的专业队伍，希望洞察能提供一个深入的视角，揭示开源世界的创新，成为启发思考的源泉。

新版的《开源态势洞察》更加专业、丰富，融入行研部门与行业各界的深入思考，形成的过程也更加开放，我们期待各界专家的共同参与。满怀期待，这本期刊能成为开源界每月必读的一本小红书。

正如同这句Slogan所言，“大家的洞察，更好的开源”。在此，我想向所有热爱开源、参与开源的朋友们发出诚挚的邀请：加入到《开源态势洞察》的共创中来，这是我们共同的“开源项目”。

开放原子开源基金会理事长

Contents

目 录

什么是开源?

作者： 适兕，王哲

导言

开源(Open Source)一词的出现,是有着明确的定义的,但是定义的高度抽象,足以让大部分人望而却步。所以笔者这里不打算从定义的解释出发,而是切换为人们的常识来看待事物。

我们常常被问及:

- 开源在我们现实生活中产生着什么作用?
- 开源能否让开发人员赚到钱?
- 开源如何走出软件产业成功“破圈”?
- 开源能为我们社会做什么?
- 我们能够为开源做什么,或者说我们做什么就算是支持开源了?我们的领导干部心里装的更多的是为人民做点什么。

相信这样的问题也真实的代表了大多数的想法,于是我们按照这样一个回答上述问题的思路来阐释和叙述开源。

开源作为信息产业中重要的一部分

开源创新的本质上是一种开放、共享、协同的创新协作模式，它依托互联网平台、通过大规模群体智慧的共同参与和协作，不断累积智慧并实现持续创新。在软件开源创新活动中，项目的核心开发人员与大规模的外围群体紧密合作，他们通过互联网来共享资源、开展协同开发、管理代码等，由此使得项目开发的效率、应对需求变化的能力大幅提升。

从狭义内涵上看，软件开源创新中的“开源”二字指的是开放源代码，软件开源创新则是指源代码开放、允许用户按照许可证条款对源代码进行修改并可自由重复发行的一类软件开发活动，

起于计算机软件行业，是一种源代码开放共享的开发模式，具有自由开放、共建共享的特性，是促进信息技术创新的重要途经。**开源软件有三个区别于专有软件（或称“闭源软件”）的核心特征：第一，允许自由分发软件，无需向创作者支付版税或许可费；第二，要求源代码与软件同时分发，或以不超过分发成本的其他方式提供；第三，允许任何人自由修改软件源代码或从中派生其他软件源代码，并根据许可证条款重新分发修改后的软件源代码。**当前的软件开源创新已经包含源代码、源数据等技术和资源的开放共享，源代码仍然是开源的主要内容。在开源模式下，通过开源许可证的方式，软件的使用者在遵守许可限制的条件下，可自由获取源代码等，并可使用、复制、修改和再发布。与此同时，虽然开源软件必须公开源代码，但需符合相应许可证的相关要求，只有在遵守许可证的条件下才能得到开源软件的源代码，并可自由地对其修改或再发布。因此，开源软件是通过许可证对其进行知识产权保护的，也是受著作权保护的作品，未经权利人许可不能随意使用。

从广义外延上看，“开源”的理念虽然诞生于计算机软件行业，但经过桌面应用、现代互联网、云计算、大数据、物联网、移动计算、人工智能等丰富的应用场景实践，开源作为软件行业创新引擎的地位不断增强，逐渐发展成强大的技术创新模式，已成为一种重要的科技创新渠道，其中产生的巨大知识增量、创新成果不仅孕育了新的软件开发方法和产品、改善了人类生活方式、改变了软件产业生态格局和商业模式，也孕育了开源文化、社区机制、大规模协作网络、开放式创新范式和创新公地理论等，其产生的影响远超出软件领域，延伸到经济社会发展的多方面[1]。因此，开源创新不仅在软件技术开发中广泛应用，还孕育了更为广泛的开放技术领域及协同创新的理念与机制，例如开放科学、开源软件、开源硬件、开源技术、开源文化、开源经济等。开源文化具有“创新、开放、自由、共享、协同、绿色、民主化”等价值取向和重要特征，即以创新为发展基轴，具有开放（开放标准、开放环境、开放源码），自由（自由发布、自由传播、自由复制、自由修改、自由使用），资源共享，协同（协同开发、协同作业、协作生产），绿色（支持绿色可再生能源、绿色环境和零边际成本效应），民主化（在协同共享中，创新和创造力的民主化正在孵化一种新的激励机制，这种机制很少基于经济回报，而更多地基于推动人类的经济生活方式，缩小收入差距，实现全球民主化）的特征。

因此，我们会发现，开源是信息技术创新的基础，是推动信息技术产业（云计算、物联网、

社交网络、移动终端、大数据、智慧城市、区块链、量子计算机和人工智能等）创新发展的重要途径和核心动力。软件开源创新的成果，已经在技术、经济和社会领域获得广泛应用，也让开源创新范式跨界进入社会科学研究者的学术视野。更进一步，相对于封闭性、标准化、强组织的创新范式，当前的软件开源创新活动强调尊重每个开发者的个人创作意愿，通过营造开放性、多元化、自组织的创作环境，充分激发大规模程序员群体的参与热情与创作灵感，通过群体智慧涌现，最终形成高水平的软件，优秀的开源软件通过互联网可以高效聚集数以万计的开发者参与贡献，其生产规模和生产效率远超任何单一商业软件公司。

2021年3月公开发布的《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》首次提出“支持数字技术开源社区等创新联合体发展，完善开源知识产权和法律体系，鼓励企业开放软件源代码、硬件设计和应用服务”，开源创新首次在中国作为国家战略被提出。此后，中华人民共和国工业和信息化部2021年11月发布的《“十四五”软件和信息技术服务业发展规划》则进一步判断开源重塑软件发展新生态，要求“十四五”期间下大气力完善繁荣国内开源生态。开源生态的构建离不开对开源创新内在机理的深刻认识与把握。

开源和闭源，或者说开放和封闭，作为软件产业的不同形态，共同为人类的生活提供服务，随着时间的累积，软件作为技术的一部分，仍然保留着技术的固有属性——维护和优化，以及不断成为迭代的基础，开源的优势越发地凸显，也就是说开源的软件形态，正在成为人类赖以生存的数字世界的重要部分，而且这个占比还在不断地上升。在HPC领域，以Linux为代表的开源项目，完全占据了排名前500的所有超算的机器。

开源作为数字时代的重要基础设施

作为现代的数字社会，软件已经是人们生活的一个重要部分，起居工作都和软件息息相关，有学者使用“道路与桥梁”来比喻数字世界的开源作为基础设施所起到的重要作用，这个比喻足以让我们明白其中原理，如果不明白的话，想想日常的塞车，人们不仅对于将节奏慢下来，充满了抱怨，更加无法想象没有道路与桥梁的世界是什么样的。

以移动互联网、云计算、大数据等现在我们的日常为例，我们每次使用一次App，都会有开源的程序在起作用，无论是运行在移动端的App（支付宝），还是远端的云计算（阿里云）服务程序，这个比例大约在70%，而且还在不断的上升。

公有云上运行的服务器操作系统，超过80%是开源的发行版：Linux，无论是简单如一次时间的校准，还是复杂如一次商品的交易，都离不开开源程序的作用。

从国家层面来看，道路与桥梁关系民生，是老百姓的大事，都投入了相应的资源来保护、建设，对应以开源软件为代表的数字基础设施也正在受到重视，以德国为例，Germany's Sovereign Tech Fund (STF) 投入资源支持开源项目的可持续性、安全性和发展前景，任何一个为我们提供日常生活相关的开源项目的不可持续，都是老百姓的灾难。中国工信部也在现有的制度下成立了开放原子开源基金会，为数字主权等开源基础设施争取更多的影响力和领导力，为老百姓的经济生活保驾护航。

开源作为大规模协作模式的组织形式

集体行动的力量，始终是我们人类不断追求的目标，无论是国家动员，还是资本公司驱动，人类集体的能力已经证明了可以制造航天飞船和万里长城这样的伟大的项目，但是能够让全球的人协作起来的项目，以开源软件为例，可谓是实现了多少人的梦想：跨越地理局限的协作，成就伟大的复杂工程。

事实上，在奥尔森《集体行动的逻辑》出版（1965年）以前，学术界普遍存在这样的假设：一个具有共同利益的群体一定会为实现共同利益采取集体行动。奥尔森认为这个假设并不能很好地解释和预测集体行动的结果，许多合乎集体利益的集体行动并没有产生。相反的，个人自发的自利行为往往导致对集体不利、甚至极其有害的结果。那么，为什么个人的理性行为往往无法产生集体或社会的理性结果？主观为自己、客观为大家的理想为什么常常无法实现？这是奥尔森思索的问题。他在本书中讲公共物品的生产分配与团体理论结合起来，讨论在“理性人”的假设下，

集体行动的特征如何，进一步涉及到如何理解个人理性与集体理性的问题[2]。

基于此，自20世纪50年代末和60年代初以来，现代经济学中兴盛发展起来了一门新的分支——公共选择理论，它研究的是传统经济学不予关心的非市场决策问题。传统经济学之所以不研究这类问题，无非是认为，诸如此类的决策和行动由于是非市场因素决定的，所以就超出了经济学有关行为的传统假定。可现代经济学的拓展和进步恰恰证明了：非市场问题并不意味着不能用经济学的方法来研究。相反，公共选择理论从它诞生的那一天起就牢牢扣住了“经济人”这个最基本的假定，认为除了参与私人经济部门活动的人之外，公共活动的参与者也受制于此，都有使自己行为最大化的倾向，无行为主体的所谓公共利益是不存在的[3]。开源是人类在信息和通信技术领域开展的极为成功的大规模集体行动协作实践，开源的成功对如何在路径多变、复杂演化的内外部条件下组织创新、实现经济社会高质量发展有战略性参考价值。

开源作为集体行动的财产再分配

大多数开源经济分析的出发点是标准的集体行动类型分析，即开源软件是非排他性和非竞争性产品，因为任何个人都可以自由修改源代码编码并将修改后的版本重新分发给其他人。那么从集体行动理论出发，上述物品的生产中所有人的最优博弈结果都是搭便车，该体系应该走向分解，但情况并非如此，现有理论无法对软件开源创新现象的经济逻辑进行全面、深入的解释。具体而言，从微观视角看，软件开源创新存续的基础来自于违背理性人假设的开发者个人行为；从宏观视角看，以价格机制为代表的市场手段和公司为代表的科层制组织形态是在复杂的分工中有效管理和配置专业知识的标准手段，但这两者在软件开源创新中都处于失效境地。软件开源创新过程较好地平衡了知识生产成本和创新收益。

当代大众熟悉的计算机软件的生产通常是知识产权制度下开展的。例如，用户可以购买微软Windows操作系统的使用权，但版权制度保护Windows操作系统不能被用户复制、修改、改进或将已购版本重新分发给他人。与此同时，大多数软件开发人员也不发布其源代码，即软件编程语言中的指令列表，因为源代码是专有软件的精髓，也是其商业秘密，专有源代码是微软能够以非

零价格出售Windows的根本原因，为了激励受雇佣的程序员创新，微软将一部分因软件专有获取的垄断租金分配给编写代码的程序员。

但是，软件开源创新活动颠覆了上述逻辑，是经济学家眼中极为“异常”的现象。开源软件的本质是源代码“自由”，软件开源创新是计算机软件源代码自由获取和传播的软件创作过程，其创作者通过开源许可证赋予被许可人对软件进行使用、修改和传播的自由。因此，软件开源创新本质上是开放的、公开的、非专有的，开源软件随源代码一起发布。开源软件有三个区别于专有软件的核心特性：第一，允许免费重新分发软件，无需向作者支付版税或许可费；第二，要求源代码与软件同时分发，或以不超过分发成本的其他方式提供；第三，允许任何人修改软件或从中派生其他软件，并根据相同条款重新分发修改后的软件。目前，全球最大的开源代码托管平台是GitHub，截至2023年上半年，全球有 1 亿名开发者在使用该平台，近60%来自北美之外的地区，其中来自中国的开发者超过1000万，位居全球第二。截至2022年底，GitHub项目有超过35亿次的开源贡献，其中包括提交、问题、拉动请求等等，超过20%的开源贡献是在公共存储库中发生的。这些项目是由数以千万计的开发人员在世界各地以无组织或自组织的形式贡献推动的，他们的代码贡献没有直接的报酬或补偿；同时，与2021年相比，对私有存储库的贡献数量增加了近38%[4]。

大部分成功的软件开源创新项目一定程度上实现了对搭便车行为的利用和改造，这些现象构成对经济学领域两大主流创新模型的挑战：一是“私人投资”（Private Investment）模型，即假设创新者的回报来自私人物品和有效的知识产权保护制度，所有的未经交易的“知识溢出”都被视为对创新者预期收益的损害；二是“集体行动”（Collective Action）模型，即假设在市场失灵的情况下，创新者会为了生产公共产品而合作，生产出的产品被列为具有非排他性（non-excludability）和非竞争性（non-rivalry）属性的公共产品，经常面临“搭便车”现象导致创新成果无法被保护，创新活动无法延续。软件开源创新的成功意味着，软件开源创新“自由松散”的表象下隐藏着亟待发掘的新理论新问题[5-6]。财产权从有形的土地，到无形的软件，中间经历了非常复杂的变化，作为一次创作，零成本复制的软件，从诞生的一开始就给所有者带来了困惑，深受知识财产法律熏陶的比尔·盖茨显然先人一步看出了其中的回报，于是发表《致电脑爱好者的一封公开信》

为抓手，将延伸所有权为手段，发明了最终用户许可协议的商业模式，一本万利，铸就了整个软件的商业帝国时代。但是，对于法理上的比例原则的话，用户几乎没有任何的权利，除了用金钱换来的许可之外，这并不利于知识的传播和发明创新，只会打造垄断的市场巨怪。那么以GPL为代表的许可，则是这种强制的替代，让渡所有权利给软件的用户，不仅可以观看源代码，还可以任何修改，重新分发。但是，正如比尔· 盖茨所言：

> **你们现在所做的一切，正在阻止人们去编写好的软件。**
> **谁能负担得起无偿做专业工作？又有什么业余爱好者能够投入3个人的时间去编程，**
> **寻找所有的漏洞，为他的产品编写文档并免费发布？**

开发自由和开源软件的开发者们，作为职业的创造者，如果无法获得有尊严的生活，那一定是对我们生活的社会极大的讽刺，显然那是一个不够文明的社会，显然圈起地来以隔离为手段的商业模式并不适合数字时代的让渡权利的方式，那么开源就是将这样的问题解决摆在首位：

- 社会组织创新，缔造新的契约
- 倡导不收取许可费用的其它诸如接口请求、副本等方式的商业活动
- 成立社会非营利机构中立组织，获得募捐
- 理清项目共同体的边界，和现实世界接轨

经济增长理论：开源作为将蛋糕做大的一种方式

哲学家詹姆斯·卡斯向我们展示了世界上两种类型的“游戏”：“有限的游戏”和“无限的游戏”。有限的游戏，其目的在于赢得胜利；无限的游戏，却旨在让游戏永远进行下去。有限的游戏在边界内玩，无限的游戏玩的就是边界。有限的游戏具有一个确定的开始和结束，拥有特定的赢家，规则的存在就是为了保证游戏会结束。无限的游戏既没有确定的开始和结束，也没有赢家，它的目的在于将更多的人带入到游戏本身中来，从而延续游戏。

显然开源的经济，是无限的游戏，以操作系统 Unix 和 Linux 的市场为例，非常有力和Solid的说明这个浅显的道理。Unix自从AT&T开始收费以来，各家商业公司进入了瓜分一个静态的市场，陷入了恶性竞争的局面：彼此互不兼容，用户被供应商锁定等，而Linux不一样，从一开始就是没有限制出现的，不仅满足当前的需求，还能被定制，并在参与中获得影响力，成为商业的共赢

平台，将操作系统在过去的三十年，扩展至云计算、移动端、航天、机器人等等无限的场景中。从限性来说，隔离理论仍然是重要的基石，但是从无限的社会而言，共享才是可持续发展的道路，我们需要将整体做大，个体才能受益更多，作为对比而言，开源比闭源更具经济增长的属性。

数字技术创新影响生产要素重组，以及生产组织变迁：知识积累与经济增长的关系

数字技术创新如何影响生产要素重组、生产组织变迁，继而成为经济长期增长的核心驱动力？在数字技术创新应用日益普遍而深入的今天，对此问题的探索性回答不仅是满足数字未来想象的理论需要，也是在实践层面回应数字化转型困境的必然要求。事实上，当前我们可能正在陷入新的一轮“生产率悖论”的困扰之中。上个世纪七八十年代，与蓬勃兴起的计算机革命相伴随的，却是长期停滞的生产率，以致罗伯特·索洛在1987年即提出，“计算机在除了生产率统计数据之外的所有地方”，类似的当前，以物联网、移动互联网、云计算、人工智能为代表的新一轮数字技术创新（或称“数字化转型”）已经随处可见并受到人们的追捧，但再次停滞的生产率是否又预示着新的“索洛悖论”的到来？

直到20世纪80年代中期，上述索洛创立的新古典增长理论都居于经济增长研究的主导地位，但随着社会的前进，新古典增长理论逐渐暴露出缺陷，新增长理论出现于80年代中期，以罗默(Paul. M. Romer)为代表，罗默把增长率内生化，也叫做内生增长理论（注：保罗·罗默是新经济增长理论的主要创始人之一，是诺贝尔经济学奖的长期候选人，曾被《时代》杂志选为1997年美国最具影响力的25人之一）。罗默在1986年提出内生经济增长模型(或称为知识外溢模型、“新增长模型”New Growth Theory)，他用内生的技术来解释经济的增长，把知识完整纳入到经济和技术体系之内，使其成为经济增长的内生变量，从而成功地将熊彼特创新思想引入新古典经济学体系。罗默的主要贡献是提出了四要素增长理论，即经济增长除了受到新古典经济学所强调的资本和劳动(主要是非技术劳动)驱动外，还受到人力资本(以受教育的年限衡量)和新知识(用专利来衡量，强调创新)影响。罗默把知识看成厂商进行自愿投资于研究开发的产物，像物质资本投资一样，厂商

进行知识投资也将使知识资本的边际收益递减。为了说明即使人口增长率为零，知识积累也足以保证经济稳定增长的问题，罗默假定:知识具有充分的外溢效应，足以抵消知识资本的边际收益递减效应。这样，知识投资的边际社会收益率保持不变或递增，既然知识的边际社会收益不减，知识的积累过程也就不会中断，从而让经济能够保持稳定增长。因此，知识不仅自身具有递增的效应，而且能够渗透于资本和劳动力等生产要素，使资本和劳动力等生产要素也产生递增收益，从而推动整个经济规模收益递增[7]。

上世纪90年代罗默进一步拓展其经济增长模型，把公共知识和企业拥有的特殊技术知识看作内生变量，经济增长依赖于通用知识的共同获得，而且公共知识的溢出有益于特殊知识的产生，且并不会降低对具有严格专有性的新知识生产的激励。罗默以阿罗(Arrow)的“干中学”概念为基础，构建了以知识生产和知识溢出为基础的知识溢出模型。他假定代表性厂商的产出是该厂商的知识水平、其它有形投入(物质资本和原始劳动等)以及总知识存量(K)的函数，这样，罗默模型实际上将整个经济通过知识积累的“副产品”性质和知识存量的外部性进行了内部化。1992年，在世界银行发展经济学年会上，罗默进一步把上述思想运用到发展中国家和地区发展战略的研究中，认为能否提供和使用更多的创意或知识品，将直接关系到一国或地区经济能否保持长期增长。

总结一下以罗默为代表的新增长理论的政策主张：一是人口规模从市场规模和分工效应两个维度影响经济增长；二是技术对生产率的改善效应明显；三是知识是非竞争性产品，人口规模越大，杰出人才出现的概率就越大，数量也越多，聪明人创造的知识为所有人使用的概率越大；四是分散经营的经济不能保证科学技术的发展，因而经济增长率就会过低，政府可以通过财政来支持研究开发，以达到促进经济增长的目的。

开源作为做大经济蛋糕的大众生产模式

上一轮“索洛悖论”的解决最终依赖于信息通讯技术成本的大幅下降，以及企业信息化改造所带来效率的巨大提升——而当前数字化转型的影响却远不限于此，不仅传统企业的运行方式正在发生变化，新的生产模式、商业模式同样层出不穷，以致既有的产业划分边界日益变得模糊，而“零

工经济”等新就业形态的兴起则对传统治理框架带来了冲击。在这样的背景下，数字技术创新究竟将如何推动生产组织变迁，以及在此变迁过程中我们应该如何主动引导或选择生产组织的新结构、新模式，便成为决定我们能否突破第二次“索洛悖论”的关键问题。

探索此问题的另一时代迫切性还在于，当前我们正在经历数字化转型的“转折点”。以上个世纪末万维网的发明为起点，彼时人们对于新的数字时代的到来充满了憧憬：以开源软件、维基百科为代表的分布式生产方式的出现，既包含着大众生产、开放创新作为新生产力变革的希望，也昭示着一个更平等、更包容数字未来的可能性。但在经历二十余年的快速发展之后，分布式生产仍然仅局限于早期经典案例而并未上升为一般性生产方式得到普及，而数字平台的崛起在维系开放性的同时也带来了零工资本主义、监控资本主义等的质疑与争议。包括蒂姆·伯纳斯·李（Tim Berners Lee）、尤才·本科勒（Youchai Benkler）在内的诸多代表性人物近年来对此的集中反思，也因此反映了对于未来数字生产方式变革的新探索。

以开源软件为例，其初始定义是指源代码可以被任意获取的计算机软件，但其更具革命意义的解释来自于生产过程与管理视角。不同于集中式、科层式的软件生产过程与管理模式，开源软件以代码的开放性包容了分散参与者的多元动机，并基于自由对话、共识决策、以个体网络联系为主的小群体联盟形成了规模化集体行动。无论是就生产过程还是结果而言，开源软件都取得了巨大的成功，不仅遍布全球的程序员愿意免费且能够有效参与软件开发进程，甚至是以营利为目的的商业公司也纷纷将本具有私有产权属性的软件代码贡献给社区，更不用说Linux、Apache、Android等开源软件产品已经成长为数字世界的基础底座。在这样的背景下，我们有理由欢呼和希冀能将其拓展至更多领域以充分释放分散主体的潜在生产力，实现创新涌现和经济社会的高质量发展。例如，以开源软件为蓝本，美国政治经济学者本科勒在2004年提出了“基于公地的大众生产模式（Common Based Peer Production，CBPP）”的核心概念，试图在数字技术革命浪潮中确立起该模式与市场模式相并行的重要位置[8-10]。但遗憾的是，这种移植努力到目前为止还并没有完全成功。

开源作为软件工程的优势方式

在“软件定义一切”的时代，如何定义软件？这是一个大问题！特别是在今天，软件上升为现代社会信息基础设施，人们越来越需要通过软件定义构造复杂世界，建模、处理那些无处不在的、“人、机、物”深度融合的智能化时代要素。在计算技术发展的历史进程中观察软件开发技术的发展，我们可以看到，软件开发面对的危机一个接着一个，这些危机不仅推动了软件开发技术的发展，而且带来了软件开发理念和方法的深刻变革，我们称其为软件开发范式的变革。

软件作为一种不断迭代的人类抽象的协作技术，从一开始就有着巨大的协作难度，尤其是颠覆了工业革命以来的直觉：为了缩短工期，可以不断地增加人员，在软件工程中，得到的是完全相反的结论：

> **向进度落后的项目中增加人手，只会使进度更加落后。**

也就是说区别于传统桥梁、道路等实体工程，软件工程有其特殊性的一面，无法靠单纯的人海战术来完成一个“终极”的系统，而是呈现出实用主义的现代工程的一面：间断性地完成某一类任务，直到周边的硬件、应用升级，变成需求，然后周而复始地进行满足。毫无疑问，“尽早发布，经常发布”哲学是最佳的方式，既避免过度设计，又避免方向错误，不断地在迭代和试错中进行。

人类科技发展的历程从一定意义上讲就是在不确定的世界中获得更多确定性的过程，在这个过程中，群体智慧是获得确定性的锐利武器，是人类文明的标志。软件开发作为人类当代独特的智力活动，经历了从作坊式的个体创作到工业化生产，再由工业化生产回归群体创作，产生了两次范式变革[11]：

（1）工程范式聚焦线性的确定性问题的软件开发，几乎放弃对不确定性问题的关注；

（2）开源范式全面拥抱不确定性，但对结果不做确定性承诺。这两次范式变革反映了人类对世界的两种科学认知，即机械论与演化论。

在“人-机-物”日益融合的三元世界中，计算平台的泛在化必然驱使软件应用的泛在化，软件定义一切预示着在不久的将来软件必将更加全面渗透人类社会方方面面，也将孕育新的软件开发

范式向开源的群智范式的最新变革（表1）。未来的软件开发需要新的科学观的指引，同时，软件定义的世界给了人类认识世界的新手段。软件创作与生产活动轨迹将演变为“参与生态、留下痕迹、形成智能、指导实践”的循环模式，人机共融的群智软件开发从必然王国逐渐走向自由王国。

表1 三次软件范式变革基本理念的对比[11]

元素		工程范式	开源范式	群智范式
		自上而下，逐步求精	自下而上，关联演化	**宏观演化，局部求精**
理念	需求	有明确用户和明确一致用户需求描述，这是软件开发的前提	没有明确的用户，开发者基于自己的构思创作软件源代码	有**潜在**用户群体，基于原型体验**发现用户**，**引导**用户需求
	质量	源代码满足需求规格的程度	开发社区的规模和口碑	软件社区关注度和口碑
	效率	开发满足需求软件的时间和成本	响应开发社区问题的时间	激发更多参与者做出贡献的效率，以及汇聚广大贡献者才智的效率
方法	过程模型	瀑布模型、敏捷模型、能力成熟度模型	开发者社区的自组织模式	激发与汇聚模型
	支持工具	软件产品线工具集	版本控制工具、缺陷追踪工具	激发与汇聚工具集
	计算环境	面向计算机环境	面向互联网环境	面向人机物融合环境

在亲力亲为中学习：开源作为人才的筛选

在企业支持开源的首要原因：招募优秀的软件开发人才！软件开发是一门实践性极为强的技术工程，传统学校走出来的学生，如果走向一线工作，需要花大量的时间和资源进行培养，这个周期少则半年，长则2年，对于在激烈竞争市场上的商业公司来说，这个周期确实是过于长了。

然而从开源项目共同体中找到的人才则恰恰相反，已经在实际中运行的代码就是最好的“简历”，不需要任何的过渡期，直接上岗，甚至如果是项目中声誉颇高的维护者能够吸引更多的开发者加入到公司来，这为企业不仅节省了培养的资源，也为上市缩短了周期。

但是企业是无法做到社会中立的组织的，天生就是为利润而来的，在市场中充满了竞争对手的不信任，也就是说开源项目共同体，即使是企业自己去构建和运营，也无法完全获得来自社会的信任。也就是说企业需要通过其它的通道来支持，例如成为开源软件基金会的成员。

关于在开源项目中成长的科学理论已经相当成熟，有很多科学家论证过：

1. 美国经济学家阿罗（Kenneth J．Arrow）的经济学理论，主张在干中学习，从而将人力资本作为生产要素之一纳入经济学研究[12]；

2. 北京大学路风教授，指出知识积累与制度创设的相互作用关系体现了生产力与生产关系、经济基础与上层建筑之间的相互作用关系，知识创新不仅事关能力积累，更是艰苦卓绝的制度创设过程，提出应重视隐性知识的积累[13-14]；

3. 马奇（James Gardner March）、西蒙（Herbert Alexander Simon）等计算科学与组织行为学者证明了，开源对于“打破”铁笼的必要性和可行性，即以实现个人利益最大化为目标的快速学习者，并不一定有利于组织知识的积累；组织成员的固化将引发组织生命力的退化；坚持对新事物新可能性的探索，可能为组织带来发展机遇；在高度竞争环境中，与趋同化相比，追求多样性的开源组织反而可能笑到最后[15-16]。

4. Frank Nagle 教授的研究成果：在亲力亲为中学习——通过贡献众包公共产品获得竞争优势

开源是人类社会为匠人们提供亲手操作的大试验场地，只要愿意付出时间和心血，总是能找到更多尚未完成的事情做，而这也成就了绕过传统选拔和筛选方式的优秀开发者的兴趣和爱好，另外，基于互联网的协作，不局限于地理位置，也让开发者能够跨越各类障碍，而在一些相对非常小众的项目上，找到开发者进行合作开发。

开源世界是培养和选拔真实人才的重要环境，其在所有人看得见的地方工作、同行评审、透明、机制清晰、以技术为最高准则等方式，吸引了大批的开发者、工程师等人才，这里也是构建人才高地的重要空间。

开源作为事实上的开放标准

开放标准对于人们的日常实在是太重要了，这一点再怎么强调都不为过。当然，有的时候，非专业的人士可能无法注意到具体的细节。

大家可以想一下自己每天上网浏览各类网站和信息的时候，是否知道 WWW 这个组织为我们提供的开放标准了呢？又或者是知道Firefox这样的浏览器的具体实现了呢？

以Linux、Kubernetes等这样的系统就起着事实上开放标准的作用，这些标准区别于通信网络等方面的标准，因为这些项目是以实际运行在生产环境中，然后将实现写下来，进而被大众认可的一类标准，而不是学术、企业、政府等机构的专业标准制定员们坐下来商量出来的。也就是说以开源项目为代表的标准是一种事实上的标准。

标准对于厂商的兼容性非常重要，无论厂商如何实现，但是需要满足消费者能够认可的统一的方式。这一点无疑开源做到了。

创造更大生态价值：开源如何“破圈”并搭建吸引力系统

网络热词“破圈理论”，其实可以深入浅出地解释开源创新活动的价值逻辑。所谓“破圈”，是搭建一个吸引力系统，像漩涡一样，把外部的人自外向内地吸引进来。换句话说，“破圈”不是你闯进别人的圈子，而是别人被你吸引，走到你的圈子里来。开源项目发展要义就是搭建一个吸引力系统，形成“注意力”漩涡或“兴趣”漩涡或“利益”漩涡，把外部的人自外向内地吸引进项目社区，并稳定在项目社区中。

怎样才能搭建一个吸引力系统？我们引入两个方便理解的关键词：“祭品效应”和“巫师-麻瓜结构”。所谓“祭品”，是你为了吸引用户，牺牲自己当下的利益，吃了一个明显的“亏”。吃的这个“亏”，就是你摆出来的“祭品”。接着，在用户当中，有人发现了你吃了亏，并且因此对你产生了强烈认同，甚至是产生了“鄙视链”，他认为自己比其他人更懂你，这就在用户中产生了“巫师-麻瓜结

构”。“开源代码”就是开源项目的原创者牺牲自己当下的利益，吃了一个明显的“亏”，就是“祭品”。开源项目的核心开发团队和外围加入的开发者围绕开源项目协同开发，并开放协同开发活动，如同“巫师”围绕祭品跳舞，吸引更多的“麻瓜”围观者，吸引力系统就形成了。

一个开源项目能否成功首先就是要看“开源代码”能否产生“祭品效应”，其次就是要看“开源协作”能否产生“巫师-麻瓜结构”。

·在1990年代，Windows操作系统让个人计算机用户感受到操作系统的价值，因为Windows是闭源的，导致Linux开放操作系统源代码产生了“祭品效应”，Linus Torvalds似乎牺牲自己当下的利益，吃了一个明显的“亏”，因此很快吸引一大批追随者，形成了“巫师-麻瓜结构”；

·2010年前后，云服务价值被广泛接受，开源云计算平台就有了“祭品效应”，并形成“巫师-麻瓜结构”；

·2015年前后，深度神经网络的机器学习价值被广泛接受，开源机器学习平台就有了“祭品效应”，并形成“巫师-麻瓜结构”。成功的开源项目必须以项目的意义被广泛接受为前提，这样的“开源项目”才能有“祭品效应”，之后，核心开发者的持续版本更新才能形成“巫师-麻瓜结构”，成为活跃社区。

·2020年至今，我们迎来了生成式语言大模型的产业爆发周期，以Meta开源LLaMA为节点，基于开源框架打造的语言大模型及其应用生态，将成为开源“破圈”的革命性里程碑。

到目前为止，全球开源生态中有影响力的开源项目主要是美国企业和社区祭出的“祭品”，产生“祭品效应”，并形成了“巫师-麻瓜结构”，其中的“巫师”当然多为美国人，而越来越多的中国开发者和广大用户成为围绕美国“巫师”的“麻瓜”群体，成为被美国开源项目这个吸引力系统吸引的对象。“麻瓜”成就了“巫师”，对“巫师”产生了依赖，成为“巫师”收割的“韭菜”，起初不自知，觉醒时可能被“巫师”卡住了脖子，无法摆脱。

中国的开源项目还很少出现具有“祭品效应”、并形成“巫师-麻瓜结构”的“根社区”。其中的原因是多方面的：

·一是项目的（精神或物质）价值还没有被认可，不足以形成吸引力；

·二是开源项目的专业性还不高（其中包括处理开源知识产权问题），还不具有“祭品”的精致

·三是业内的“精明人”只想当“巫师”，至少十分警惕成为他人的“麻瓜”。当然，更主要的原因是价值被认可的专业软件项目核心团队没有主导群智开源范式意识和能力，不愿意吃一个明显的“亏”，没有及时祭出开源代码，因此长期不能“破圈”。

“祭品效应”和“巫师-麻瓜结构”的隐喻似乎源自宗教控制手法，以此解释开源破圈的社会心理机制具有一定借鉴意义。**但是，开源创新不是现代宗教或巫术。这里有三点需要明确被认知**：

·第一，开源不是控制参与者，而是吸引志同道合者参与创造；

·第二，开源项目的主导者不是“天赋巫师”，而是价值创造者；

·第三，“巫师”与“麻瓜”的角色不是一成不变的社会角色，而是相当于特定开源项目的暂时角色，同一个人，既可能是一个开源项目的主导者（即“巫师”），也可能是另一个开源项目的参与者（即“麻瓜”）。

本章小结

开源已经成为近20年来最具活力的技术创新模式，全球开源创造生态网络成为全球技术生态网络发育最迅猛的部分。开源创造首先在软件开发领域获得成功，进一步进入芯片设计、工业设计以及文化创意等领域。**开源产业欣欣向荣，企业巨头纷纷入场。**谷歌掌控了基于Linux内核的智能手机操作系统Android，全球82%的智能手机使用该操作系统；2018年10月28日，IBM以340亿美元收购了全球最大的基于Linux的服务器操作系统服务商RedHat；微软公司于2018年6月4日收购了全球最大的开源平台GitHub，标志着微软这个当年与开源软件势不两立的传统软件巨头全面拥抱开源创造，2019年6月30日微软市值突破一万亿美元，20年来再回世界市值第一宝座。**开源创造生机勃勃，开源创造平台功不可没。**当前，10年来在GitHub上托管的源代码数量约20TB，已经与3000多年人类文明产生的文字文献数量相当，在GitHub上注册的开发者人数已经超过全球在软件企业工作的程序员的数量，90%以上的软件开发者认为开源加速了创新[4]；GitHub平台上不仅有以Linux操作系统内核为代表“明星级”开源项目，而且集聚了一大批包括主流深度学习框架在内的各类新兴领域的开源项目。

让我们回忆一下经济学家和历史学家解释工业革命时的理论，几乎没有将注意力放在蒸汽机的具体实现上，而是聚焦在围绕蒸汽机发展出来的一整套知识财产权保护体系和交易保障。如果我们能从这个思路去进行下去的话，开源所代表的现代数字秩序，显然也并不是具体的计算机语言如何解决一个问题，而是围绕这个协作起来的创造者们能够在创新进步的同时获得有尊严的回报，这亦是一个社会经济思考范式的转变。

软件驱动着人类进步，而开源在其中是起着重要作用的一种形态，但是，历史和我们开了一个大大的玩笑，闭源的形态更加符合人们的直觉，占据了一部分人的心智，尽管它将权力伸进了人们的卧室，所幸的是，随着软件作为技术的积淀，开源的优势，尤其是对于中国这样的后发国家，才刚刚显示出来。

回顾开源发展历史，我们可以清晰地看到，开源创造缘起上世纪80年代美国程序员群体的“自由软件”运动，其价值观源自学术界自由表达与平等交流的传统，以及程序员群体中共创共享源代码的传统。“自由软件”开源创新逻辑与那个时期蓬勃发展的软件产业保护程序源代码的商业逻辑产生了严重对立。到上世纪90年代末期，“开源软件”概念被提出，实现了基于众包的创新模式和基于服务的商业模式的平衡，开源创造蓬勃发展。

开源软件的创新逻辑是，通过开源，以更高的效率汇聚更多的“创客”，参与到新技术的革新和发育之中，以寻求实现技术突破。**开源创新的商业逻辑是也是通过开源，以更低的成本吸引更多的“新潮”用户，参与到新产品的成熟和传播之中，以寻求迅速从边缘低端产品变成主流高端产品。开源协作的经典模式是，**发起人（类比为“编剧”，可以是自然人，也可以是商业公司或非营利性基金会），在开源创造平台（类比为“剧场”）上发布开源创造项目（类比为未完成“剧目”），汇聚创客（类比为“写手”或“群演”），吸引用户（类比为“观众”）。总而言之，开源软件为我国获得并学习主流基础软件核心技术、提高自主创新能力提供了新途径，开源创新模式已经成为我国技术创新能力升级的新途径[17][18]。

由此可见，开源并不是孤立的一个个软件项目，而是现代世界的信息产业的一部分，你可以无视它，但你不能没有它。当然，数字时代的新事物，就需要有对应的新的制度来维护其可持续发展，而这需要全社会的努力，需要政府、智库、企业、科研院校、法律系统、消费者等等通力合作，方有可能结出累累硕果。在中国，领导干部有着至关重要的举旗定向作用，加深对开源的认识更为重要。

参考资料来源（王哲部分）

[1]Ostrom, E. (1990). Governing the Commons: The Evolution of Institutions for Collective Action. Cambridge University Press.

[2]Olson, M. (1989). Collective action. In The invisible hand (pp. 61-69). London: Palgrave Macmillan UK.

[3]von Hippel, E., & von Krogh, G. (2003). Open source software and the "private-collective" innovation model: Issues for organization science. Organization Science, 14(2): 209-223.

[4]https://github.blog/2023-01-25-100-million-developers-and-counting/

[5]Von Hippel, E., (2001). Innovation by user communities: Learning from open-source software. MIT Sloan Management Review, 42: 82-86.

[6]Von Krogh, G., S. Haefliger, S. Spaeth, and M. W. Wallin. (2012). Carrots and Rainbows: Motivation and Social Practice in Open Source Software Development. MIS Quarterly, 36(2):649-676.

[7]Romer, P. M. (1987). Growth based on increasing returns due to specialization. The American Economic Review, 77(2), 56-62.

[8]Benkler, Y.(2002). Coase's penguin, or Linux and the nature of the firm. The Yale Law Journal (112): 369-446.

[9]Benkler, Y.(2006). The Wealth of Networks: How Social Production Transforms Markets and Freedom. New Haven and London: Yale University Press.

[10]Benkler, Y. (2013). Practical anarchism peer mutualism, market power, and the fallible state. Politics & Society, 41(2), 213-251.

[11]王怀民, 余跃, 王涛, 丁博. 2023. 群智范式: 软件开发范式的新变革[J]. 中国科学: 信息科学, 53: 1490-1502.

[12]Arrow, K. J. (1969). The Organization of Economic Activity: Issues. The Analysis and Evaluation of Public Expenditures: the PPB System: pt, 1.

[13]路风, & 封凯栋. (2004). 为什么自主开发是学习外国技术的最佳途径?——以日韩两国汽车工业发展经验为例. 中国软科学, (4), 6-11.

[14]路风, & 余永定. (2012). "双顺差", 能力缺口与自主创新——转变经济发展方式的宏观和微观视野. 中国社会科学, (6), 91-114.

[15]March, J. G. (1991). Exploration and exploitation in organizational learning. Organization science, 2(1), 71-87.

[16]Simon, H. A. (2013). Administrative behavior. Simon and Schuster.

[17]王怀民院的演讲:《开源创新的启示》

——5月26日至5月30日，2023中关村论坛举行期间，中科院院士、CCF开源发展委员会主任王怀民教授发表了关于"开源创新启示"的演讲（https://new.qq.com/rain/a/20230530A0ATZB00）

[18]老石谈芯对王怀民院士的专访节目:https://www.bilibili.com/opus/763143224043765842

专题：CRA引发巨大争议，开源安全何去何从

——开源领域网络产品和服务的网络安全法律规制

*Resilience：n. 韧性、复原力、恢复力、弹性、回弹性、还原能力、快速恢复的能力、适应力

序言：

据欧盟研究报告表明，仅在2021年一年，全球软硬件产品的网络安全犯罪就造成了5.5万亿欧元的损失。在联网环境下，一种数字产品的网络安全攻击，可能会影响整个组织和整个供应链，并可在几分钟内跨境传播至整个欧盟内部市场。正可谓，“如果万物互联，则万物皆可被攻击。”欧盟意识到，只有在整个供应链中所有组件都安全时，整个供应链的网络安全才能得以保障。2022年9月15日，欧盟委员会的《网络韧性法案（CRA）》提案应运而生。

CRA提案一经公布，就引发了全球开源圈的热议。特别是今年7月份欧盟议会对Recital 第10条“开源豁免条款”的修正意见，更是激起了多家开源基金会及社区的担忧甚至是谴责，但相关建议并未被采纳。基于欧盟立法分工及流程，当前CRA提案已进入Trilogue阶段（欧委会、欧盟议会、欧盟理事会的三方会谈）并旨在就待决问题形成临时议定。而这一政治敏感阶段距离CRA提案的最终生效已然咫尺之遥，留给制造商等经济运营体的合规过渡期也并非宽裕，那么开源安全将何去何从？

本专题邀请了来自产业界、法律界的专家，从不同维度出发共同探讨在全球视野下，开源软件在现行/拟议的网络安全立法中是否受到调整、如何界定调整边界以及将造成何种影响等议题。

扫描下方二维码，浏览CRA最新立法文本及其译文

CRA拟施加的安全义务与开源

撰稿：Vanessa 开放原子开源基金会
vanessa@openatom.org

立法背景：

网络安全是欧盟委员会的首要任务之一，也是数字化和欧洲互联的基石。据欧盟研究报告表明，仅在2021年一年，全球软硬件产品的网络安全犯罪就预估造成了**5.5万亿欧元**的损失。在特定条件下，任何集成在更大的电子信息系统中或与之相连的具有数字元素的产品都可以成为恶意行为者的攻击媒介。这既包括通过硬件接口进行物理连接的产品，也包括通过网络插座、管道、文件、应用程序编程接口或任何其他类型的软件接口进行逻辑连接的产品。为了确保一个更有网络韧性的欧洲，此前，欧盟已发布了**《2020年欧盟网络安全战略》和《2020年欧盟安全联盟战略》**两个战略，也建立了包括《网络和信息系统安全指令》(NIS指令)、最近由欧洲议会和理事会通过的《全联盟高共同水平网络安全措施指令》(NIS2指令)以及《欧盟网络安全法案》等内容在内的**欧盟网络安全框架。**[1]

2022年9月15日，针对当前硬件和软件产品越来越容易受到网络攻击的问题，**欧盟委员会(European Commission进一步持续公布了《网络韧性法案》（Cyber Resilience Act，以下简称为“CRA”）提案[2]，该提案核心目标包括：确保制造商从设计和开发阶段开始以及整个产品生命周期内改善投放到欧盟市场的具有数字元素的产品**（包括任何软件或硬件产品及其远程数据处理解决方案，包括单独投放市场的软件或硬件组件）**的网络安全性**。该提案将完善欧盟网络安全规制框架。

当前，经过今年7月份欧洲理事会(European Council)、欧盟议会（European Parliament）各自表决及各自修正，CRA提案正处于欧盟委员会、欧洲理事会、欧盟议会的Trilogue（三方会谈）阶段，预期在2024年正式生效。

[1] https://ec.europa.eu/commission/presscorner/detail/en/IP_22_5374

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454

合规义务：

该提案拟规定，全球的软硬件数字产品投放到欧盟市场前要通过自查或第三方检查，确保满足欧盟网络安全标准，并由欧盟颁发“CE”标识后才能投放到市场，以解决已识别的漏洞，以确保消费者和用户免受安全功能不足的产品侵害并充分知悉其购买的产品的安全信息。为此，该提案要求每个**成员国**至少任命一个市场监督机构以确保CRA的有效实施，并约束了包括制造商[3]、进口商、分销商等在内的**经济运营体（economic operators）**的不同义务，分列在包括8章节、57条款的正文，以及6个附件之中。**应先判断是否构成CRA提案项下的经济运营体，再审视应履行的义务。**原始提案版义务如下:

经济运营体	**制造商**	义务包括但不限于：按照安全要求[附件1]进行安全评估[附件6]并获取CE标识、全程技术文档记录[附件5]、上市后5年/产品生命期的安全漏洞处理（乃至召回）及向欧盟通报等义务，且制造商应指派**授权代表**配合相应监管和执法。此外，如果进口商和分销商以其名义或在其商标下或进行**实质修改**后再次投放已投放市场的产品，则**视同制造商**。（其他主体实质修改，也要对其实质修改的地方负责）
	进口商	义务包括但不限于：仅能将制造商已完成安全合规并有CE标识的产品投放到欧盟市场，如识别到安全漏洞等网安风险应通报制造商解决及市场监管主体（如涉及重大风险）。此外，进口商还应在投放市场10年内保留欧盟合规声明副本，以供监管机构使用。
	分销商	分销商应在产品投放市场前，检视该产品是否已有CE标识，制造商、进口商是否已分别遵守义务，如发现网安问题应即使通报制造商解决及市场监管主体（如涉及重大风险）。
	识别经济运营体	所有以上经济运营体均应留存10年其产品的供应商或供应对象的名称及地址。

[3] 制造商：开发或制造或委托开发制造“具有数字元素的产品”，并将其以其名义或在其商标下收费或免费投放到市场的主体。

本提案附件I所述的制造商等应遵守的**核心网络安全要求**为：

1\具有数字元素的产品的特性有关的安全要求		**2\安全漏洞处理要求** 具有数字元素产品的制造商应当：	
(1)	具有数字元素的产品的**设计、开发和生产**，应确保根据风险达到适当的网络安全水平；	(1)	确定并记录产品中包含的漏洞和组件，包括以常用的、机器可读的格式**起草一份软件物料清单(SBOM)**，至少涵盖产品的最高级别依赖关系；
(2)	具有数字元素的产品**在交付时应不存在任何已知的可被利用的漏洞**；	(2)	关于对具有数字元素的产品构成的风险，**毫不延迟地处理和修复漏洞**，包括提供安全更新；
(3)	根据第10(2)条所述的**风险评估**并在适用的情况下，具有数字元素的产品应:	(3)	对具有数字元素的产品的安全性进行有效的定期测试和审查；
	(a) 在交付时采用安全的默认配置，包括可以将产品重新设置为初始状态；	(4)	**一旦提供了安全更新，就公开披露有关已修复的漏洞的信息**，包括对漏洞的描述、允许用户识别受影响的数字元素产品的信息、漏洞的影响、其严重性以及帮助用户修复漏洞的信息；
	(b) 确保通过适当的控制机制，包括但不限于认证、身份或访问管理系统，防止未经授权的访问；	(5)	制定并执行有关协调漏洞披露的政策；
	(c) 保护存储、传输或以其他方式处理的个人或其他数据的机密性，例如通过最先进的机制对静止或传输中的相关数据进行加密；	(6)	采取措施，促进共享有关其具有数字元素的产品以及**该产品中包含的第三方组件的潜在漏洞的信息**，包括提供一个联系地址，用于通报在具有数字元素的产品中发现的漏洞。
	(d) 保护存储、传输或以其他方式处理的个人或其他数据、命令、程序和配置的完整性，防止未经用户授权的任何操纵或修改，并报告损坏情况；	(7)	提供安全发布具有数字元素的产品更新的机制，以确保可利用的漏洞得到及时修复或缓解；
	(e) 仅处理与产品预期用途相关的充分、相关和必要的个人或其他数据（"数据最小化"）；	(8)	确保在有安全补丁或更新来解决已发现的安全问题时，**毫不拖延地免费发布这些补丁或更新**，**同时向用户提供咨询信息**，包括可能采取的行动等有关信息。
	(f) 保护基本功能的可用性，包括抵御和减轻拒绝服务攻击；		
	(g) 尽量减少自身对其他设备或网络所提供服务的可用性的负面影响；		
	(h) 在设计、开发和生产时限制攻击面，包括外部接口；		
	(i) 在设计、开发和生产时使用适当的利用缓解机制和技术减少事件的影响；		
	(j) 通过记录和/或监控相关内部活动，包括数据、服务或功能的访问或修改，提供与安全相关的信息；		
	(k) 确保通过安全更新，包括在适用情况下通过**自动更新和通知用户**可用的更新来解决漏洞。		

此外，**CRA提案将具有数字元素的产品[4]区分为“产品”和“关键产品”**[附件3]，**以反映与这些产品相关的网络安全风险水平；**其中**关键产品**又包含Class Ⅰ、Class Ⅱ两类，其中涵盖操作系统、浏览器、密码管理、VPN、网络管理、防火墙等相关软件种类。同时，该提案规定**“产品”**自行评估即可，但**“关键产品”**的开发者不可以通过自我评估的方式履行合规义务，**而是需要引入第三方CE标识审计师进行审查以履行合规义务。**Class Ⅰ和Class Ⅱ涵盖的数字产品具体如下：

Class Ⅰ	Class Ⅱ
1. 身份管理系统软件和特权访问管理软件；	1.用于服务器、台式机和移动设备的操作系统；
2. 独立和嵌入式浏览器	2.支持虚拟化执行操作系统和类似环境的管理程序和容器运行系统
3. 密码管理器	3.公钥基础设施和数字证书发行机构
4. 搜索、删除或隔离恶意软件的软件	4.工业用防火墙、入侵检测和/或防御系统
5. 具有虚拟专用网络（VPN）功能的数字元素产品	5.通用微处理器
6. 网络管理系统	6.用于集成可编程逻辑控制器和安全元件的微处理器
7. 网络配置管理工具	7.工业用路由器、用于连接互联网的调制解调器和交换机
8. 网络流量监控系统	8.安全元件
9. 网络资源管理	9.硬件安全模块（HSM）
10. 安全信息和事件管理系统（SIEM）	10.安全密码处理器
11. 更新/补丁管理，包括启动管理器	11.智能卡、智能卡阅读器和令牌
12. 应用程序配置管理系统	12.供[第XXX/XXX (NIS2)号指令附件一]所述类型的基本实体使用的工业自动化和控制系统 (IACS)，如可编程逻辑控制器 (PLC)、分布式控制系统 (DCS)、机床用计算机数字控制器 (CNC) 以及监控和数据采集系统 (SCADA)；
13. 远程访问/共享软件	13.供[第XXX/XXX 号指令（NIS2）附件一]所述类型的基本实体使用的工业物联网设备；
14. 移动设备管理软件	14.机器人传感和执行元件以及机器人控制器
15. 物理网络接口	15.智能仪表。
16. 不属于第二类的操作系统	
17. 不属于第二类的防火墙、入侵检测和/或防御系统	
18. 路由器、用于连接互联网的调制解调器和交换机（不属于第Ⅱ类）；	
19. 不属于第Ⅱ类的微处理器	
20. 微控制器	
21. 供[第XXX/XXX 号指令（NIS2）附件一]所述类型的基本实体使用的专用集成电路 （ASIC）和现场可编程门阵列（FPGA）；	
22. 不属于第二类的工业自动化和控制系统（IACS），如可编程逻辑控制器（PLC）、分布式控制系统（DCS）、用于机床的计算机数字控制器（CNC）以及监控和数据采集系统（SCADA）；	
23. Ⅱ类未涵盖的工业物联网。	

[4] 在具有数字元素的产品范围上，该提案不适用于《人用医疗产品及配件的欧盟条例[EU]2017/745》《人用体外诊断医疗器械及其配件的欧盟条例[EU]2017/746》《民用航空安全的高度统一水平的欧盟条例[EU]2018/1139》以及《机动车辆及其挂车，以及用于此类车辆的系统、部件和独立技术单元的型式批准要求的欧盟条例[EU]2019/2144》下的相关产品。

该提案一经生效，经济运营体和成员国将有**2年**过渡期来完成CRA合规遵从，履行对积极利用的漏洞和事件的通报义务的制造商则将仅有**1年**过渡期。此外，相关法定义务处罚相当严厉：如果未能履行CRA附件1和第10、11条所施加的义务，则将处以**最高1500万欧元**或上一财年全球年度营业额的2.5%的行政处罚，不履行其他义务的将处以**最高1000万欧元**或上一财年全球年营业额的2%的行政处罚。如果向市场机构提供不正确、不完整或误导性的信息，将被处于**最高500万欧元**或上一财年全球年营业额1%的行政处罚。

与开源的关系：

问题1：开源项目/行为是否落入CRA调整范围内？

欧委会(Commission)的CRA提案在Recital 10中对软件开源设置了例外条款，称“为了防止阻碍创新和研究，在‘商业活动’过程之外开发和提供的自由和开源软件将不被该草案覆盖”，并提别提示，**“商业活动”不仅是对软件收费，对于对技术支持收费、提供软件平台对其他服务收费，或者在提高软件安全性、兼容性或互操作性目的之外使用个人数据，**均为商业活动。

欧盟理事会(Council)对CRA提案的修正案[5]欧盟理事会于今年7月13日在其修正案中新增几个观点，包括但不限于：（1）“商业活动”指的对产品收费、对技术支持服务收费、通过其他收费平台等，**且在确定活动的商业或非商业性质时，不应考虑产品开发的情况或开发的融资方式。此外**，促进软件开发和供应的**软件包管理器、代码托管或协作平台**只有在将该软件投放到市场上并因此在欧盟市场上提供分发或使用时才被视为**分销商**。基于前述要素，在“商业活动”中提供开源软件则将受该提案调整[Recital10]；（2）制造商应识别数字元素产品的组件（包括开源组件）中的安全漏洞，并向组件维护者通报[Art11.7]。

欧盟议会(Parliament)对CRA提案的修正案[6]：欧盟议会基于ITRE committee的意见/Opinion于今年7月26日发布了修正案，该修正案对开源的态度更为激进。该修正案新增了包括但不限于如下观点：

（1）开源产品是否作为商业活动的一部分提供应个案评估，关注具有数字元素的开源产品的**开发模式及供应阶段**。

[5] https://data.consilium.europa.eu/doc/document/ST-11726-2023-INIT/en/pdf

[6] https://www.europarl.europa.eu/doceo/document/A-9-2023-0253_EN.html

例如：1.开源项目的主要开发者是来自单一主体的的雇员或committer来自于单一主体，那么被视为商业活动，**除非其是“完全去中心化的/fully decentralised”开发模型（即没有单一公司主导项目代码）**；2.任何经常性地接受了商业公司资金捐赠的开源项目将被视为商业活动；3.绝大多数打包管理器、代码托管协作平台不被视为本法案的分销商[Whereas10-10e]；

（2）对于开源软件，**制造商中立的非营利组织**、独立开发者通常不受本法案调整，但鼓励按照Annex1进行合规 [Recital 9a]；

（3） **仅**在商业活动中**被用为商业产品**的自由开源软件受到调整，**制造商**被视为向市场**商业性供应**产品的的主体 [Recital 10]；

（4）制造商应对引入的三方来源组件形式尽职调查，在引入并**非换取经济价值**的三方开源软件情形下，制造商也确保尽调合规 [Recital 32a]；

（5）无论是否能修复，所有安全漏洞必须及时（24h）报告给ENISA（欧盟网络安全机构）及该组件的维护方 [Recital 35]，但**这只是制造商的义务并非开发者的义务** [Art11 p.7]。

通过比对上述几个版本可以看出，欧盟拟通过“商业活动”的定义来限定“投放到欧盟市场的产品”。在这个定义下，看似意在豁免开源行为实则旨在规制，**并通过多重限定覆盖了主导开源、参与开源和使用开源的大部分场景，**而这也符合立法目的及现有立法框架。在文本上，实际立法者欧盟理事会的版本看似表意更模糊，或许能够为开源豁免留有更大余地，尽管CRA尚未定稿，但开源领域的强安全规制已然势不可挡。

不过，联合立法者欧盟议会的版本中所提到的“制造商中立的非营利组织”以及“完全去中心化”的开发模式，因多种原因（例如，开源项目可持续性考量、开源项目治理的成熟度问题、被动作为开源项目发起方商业闭环的中间角色）对于开源基金会来说并非完全是实然状态，因而未完全排除非营利性开源基金会。

问题2：开源主体履行CRA义务的影响是什么？

鉴于在绝大多数软件中包含开源组件，CRA对于开源界的影响是广泛且深远的。开源主体/行为落入该法调整范围后，那么安全评估义务最为严苛的“关键产品”将会覆盖大量开源项目，包

括但不限于**操作系统、浏览器、面向特定实体的ASIC和FPGA、安全加密处理器、机器人控制器、工业物联网等各方各面的开源技术。**

早在2022年欧委会发出提案时，即有18家涉及开源的慈善机构、商业社团及公司就CRA提案的审议及通过是否以及如何对开源生态产生影响向欧盟委员会表达了顾虑与担忧，并就基于开源行业维度对CRA提案提出建议[7]欧盟议会的上述表态[0726]更是让包括Eclipse基金会[8]、Mozilla基金会[9]等开源基金会感到悲观。

海外基金会提出的相关影响及难点包括但不限于：

（1）**开源安全漏洞处理方式受到影响**：该提案中设置了发现安全漏洞、任何影响安全的事故的24小时内向ENISA的通报机制。当前开源社区的安全漏洞处理实践各不相同（例：某项目在漏洞未修复前不得在社区层面去公布和传播，外采工具在社区自动提交安全pr，以**发版**为截点进行闭环；某项目采用国际标准（ISO/IEC 30111、ISO/IEC 29147）规范其安全性；Eclipse/所有漏洞都要披露社区但自行决定是否上报官方机构）。**OpenSSF**也曾就此给出了包括“应参考安全漏洞的影响、处理及汇报等方面的业界最佳实践”、“欧盟政策制定在考虑适用于软件开发的法规时应咨询开源社区及其安全最佳实践”在内的八点建议[10]，作为对CRA提案的补充。

（2）**对于发版频繁、项目繁多的开源基金会将难以实施或拖垮项目。**假设**开源基金会**400个项目每年各发版4次，那么在项目发版/Release时至少需进行1600次安全检视，并对正式版本进行CE标识认证，测试版本应标识其不符合本条例，且基金会作为制造商应积极监管该安全合规，而非被动收悉结论归档。

（3）**开源基金会无法知道谁（用户）以及哪种应用场景下使用了其代码**，被下游纳入到了何种产品中，在遵守“call home”机制向下游用户进行无延迟地安全漏洞信息更新的同时可能存在困难。

（4）**系列连锁反应**：由于合规遵从是在产业链、供应链中传导的，一旦CRA生效，开源社区/开源商业公司/开源基金会将可能对开发者施加安全义务以完善开源项目的合规流程，这可能会削弱本就无偿劳动的独立开发者对于基金会维护项目的参与积极性。此外，非欧盟的开源基金会及项目进入欧盟义务加重，可能会使得对在欧发展开源项目时怀有更多顾虑，甚至造成社区分裂。最终可能有违其Recital10条所述的不破坏欧盟市场创新活力的初衷。

[7] https://blog.opensource.org/the-ultimate-list-of-reactions-to-the-cyber-resilience-act/

[8] https://www.youtube.com/watch?v=AmsM5_5QO5A

[9] https://blog.mozilla.org/netpolicy/2023/07/13/european-parliaments-version-of-the-cra-threatens-cybersecurity-and-open-source-development/

[10] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services/F3376650_en

问题3：对CRA有哪些展望？

当前，CRA立法已然箭在弦上，作者理解尽管CRA的设立将大幅提高企业、机构的义务履行成本，但更能极大减少安全攻击/缺陷所造成的产业链、供应链的损失，最终极大提高欧盟网络韧性，为全球范围内网络安全做出贡献。

此外，鉴于外部机构可能尚无路径实质影响CRA立法导向，且对欧盟立法终版是否能够澄清CRA对“从事开源公益事业的非营利组织（如某些开源基金会）”的豁免程度、以更大程度平衡安全合规义务与开源创新之间的关系尚无更多信息，作者仅在此希望CRA能够为开源场景设立个案评估机制，并提供详尽指引。

背景小知识：

欧盟立法目标及效力：

· 根据Article 26 TFUE，欧盟立法的共同目标是**实现欧盟内部市场**，即确保货物、人员、服务、资金的自由流通。

· 根据Article 288 TFUE，TFEU和TEU是欧盟的基本法。二级法律中：**欧盟条例/Regulation**在生效后直接在成员国政府、自然人/法人、法院适用；**欧盟指令/Directive**生效后仅对成员国政府直接适用，不直接在成员国自然人/法人、法院适用，而是应转化/transpose为成员国的国内法后再适用；**欧盟决定/Decision**由欧委会或欧盟理事会做出，针对特定的成员国或市场主体的法律；**建议和意见**，指导性文件。

欧盟立法目标及效力：

· 根据Article 17 TUE：欧委会European Commission由每家成员国的委员组成，代表欧盟的普遍利益，而非代表成员国利益，欧委会不得寻求或者接受成员国政府的指示，下设53个事务部门，欧委会主席在国际层面代表欧盟。**欧委会是欧盟条约的捍卫者及实施者**，确保成员国是否正确适用欧盟条例、是否将欧盟指令转化为国内法。**仅欧委会具有欧盟指令和条例的提案权**，在这个意义上，被誉为欧盟的“发动机”。

· 根据Article 16 TUE：欧盟理事会Council of EU是成员国部长一级的代表的组成，代表成员国利益，每个国家1个席位，并下设10个类别理事会。原则上简单多数（55%成员至少15个成员国且代表了65%的人口）方可通过，外交安全事项须一致通过。欧盟理事会基于欧委会的立法提案进行投票，是联合立法者但也是实际立法者，首先对提案进行修改及投票。

· 根据Article 14 TUE：欧洲议会European Parliament由议会选出的不超过750名公民代表+议长1人组成，代表成员国的公民。欧盟议会的议员不是以国家的形式形成派别，而是以政党的形式形成派别，但每个国家只能有6-96个席位。为了行使立法权、预算批准权，欧盟议会还设立了20个委员会和两个分委会，这些委员会将各自负责的事务，审议相关法律提案，提出具体意见，提交欧盟议会作出必要的决定。欧盟议会基于欧委会的立法提案进行投票，**是联合立法者**，再次对提案进行投票即可采纳，如有修改应请理事会再次投票直至双方达成共识。

译文|拯救开源:《网络韧性法案》即将带来的悲剧

作者:

Dirk-Willem van Gulik

VP, Public Affairs, ASF

译者:

刘天栋 Ted

开源社联合创始人 | ASF Member

ted@kaiyuanshe.org

原文请见https://news.apache.org/foundation/entry/save-open-source-the-impending-tragedy-of-the-cyber-resilience-act，发表于2023年7月18日

译文已发表在“开源雨林”公众号https://mp.weixin.qq.com/s/_WOrj6_CclSR5q9lkcydFA ，发表于2023年8月14日

包括开源软件在内的软件正在受到全世界的监管。这篇冗长的博文解释了欧盟《网络韧性法案》的背景、优点、缺陷以及对开源软件可能产生的负面影响。此外，它还解释了该法案在欧盟系统中的复杂流程，以帮助人们了解时间表和如何推动改变。

译者注：欧盟《网络韧性法案》https://www.european-cyber-resilience-act.com/

如果您需要更多的口头介绍，Eclipse的MikeMilinkovich提供了一个非常新颖、清晰的演示，涵盖了相同的内容。如果您更喜欢简短的行动呼吁，那么不妨试试GitHub　CNLL（法语内容）、Linux 基金会或更广泛的行业响应。

> 译者注：
> * 一个非常新颖、清晰的演示 Update on the European Cyber Resilience Act：
> https://www.youtube.com/watch?v=AmsM5_5QO5A
> * 行动呼吁：GitHub、Linux 基金会
> *GitHub：https://github.blog/2023-07-12-no-cyber-resilience-without-open-source-sustainability/
> * Linux基金会：https://linuxfoundation.eu/cyber-resilience-act
> *行业响应：https://ccianet.org/library/joint-recommendations-for-a-feasible-cyber-resilience-act/

背景小知识：

虽然与其他大型行业和部门相比，IT行业的规模还很小，但在过去的几十年里，它已成为社会的关键。现在，在新闻中经常可以看到软件和IT行业的大型事件。而且，更常见的是由某种灾难引发的故事：配置错误、漏洞或显然太容易 "进入" 的犯罪分子和国家行为。现在，不良的IT实践也影响到了主要行业，从能源运输、制造业到金融业，再到民主进程和治理良好的政府。

正因为如此，社会和各种管理机构当然也注意到了这一点，因此，世界各地都在制定各种软件管理条例和立法。

历史：

以工程史为例，这种监管是再正常不过的结果。19 世纪末，机械行业取得了惊人的发展，这在一定程度上要归功于蒸汽机的发明。但随着这一行业的发展，蒸汽锅炉爆炸事故也随之增多。这些事故通常会夷平半个城镇。

1865 年，蒸汽船Sultana号发生爆炸，造成1,167人丧生。因此，美国锅炉制造商协会（以下简称ABMA）成立，开始对该行业进行自律。经过数百次此类爆炸，以及1905年在波士顿一家鞋厂发生的一次代价特别高昂的爆炸，政府才开始采取干预政策。

有趣的是，应对1905年灾难的并不是ABMA，而是由五名工程师组成的小组，他们是美国机械工程师协会的成员，这是一个由个人而非公司组成的专业组织。这些人撰写了第一版《锅炉规范》，随后不久便得到了马萨诸塞州立法机构的认可。

从很多方面来说，这些工程师、这些个人志愿者 "自救" 来解决问题；就像我们今天在ASF的开源以及IETF（互联网工程任务组）在制定互联网标准中所做的一样。是专业团体解决了问题：而不是他们的雇主、行业或美国锅炉制造商协会。

现状：

目前，世界各地几乎都有大量立法正在进行中；美国和欧盟稍稍领先（各国决策者之间也进行了大量协调）。在这篇博文中，我们暂时只关注其中一项：欧盟的《CRA-网络韧性法案》，因为从时间轴的角度来看，这是 "先行者"。

这绝对不是最重要的立法。在ASF里，我们认为欧盟的《PLD-产品责任指令Product Liability Directive》（引入了对软件"严格责任"的规范）、美国的第14028号行政命令 "提高国家网络安全" 和 "2023年开源软件安全法案"（美国）可能会产生更大的影响。

> 译者注：
> * 美国的第14028号行政命令 "提高国家网络安全：
> https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
> * “2023年开源软件安全法案”（美国）：
> https://www.congress.gov/bill/118th-congress/senate-bill/917/text

这一点可能尤为正确，因为美国立法可以通过国家标准与技术研究院（NIST）为本国制定标准，而国家标准与技术研究院制定标准的速度通常快于欧盟制定标准的速度（因此很可能制定出全球标准）。

这种事情能做吗?

在日常实践中，软件开发人员很少需要考虑监管问题（除非TA们从事某些特定领域的工作，如医疗、航空航天、金融或核能）。开源许可证（在我们的下游）和提交者许可证协议（在我们的上游）往往有范围广泛的免责声明。我们通常将代码等同于编撰成文的知识或言论。

但在实际操作中，事情并非如此简单。例如，在ASF，我们多年来一直需要提交一些文件，让美国工业与安全局（BIS）知道我们提供下载的加密代码的确切位置[https://infra.apache.org/crypto.html]。由ASF发布的代码不能出口（或再出口）到特定目的地或特定名单上的人。

> 译者注：
> 特定目的地或特定名单上的人-出口ASF产品的规范：
> https://www.apache.org/licenses/exports/

网络韧性法案

在欧盟，《CRA-网络韧性法案》目前正在法律制定过程中（将于2023年7月19日进行关键投票）。该法案将适用于欧盟的大量软件（以及带有嵌入式软件的硬件）。该法规的初衷是好的（也可以说是早该如此）：使软件更加安全。

> 译者注：欧盟《网络韧性法案》https://www.european-cyber-resilience-act.com/，已经投票通过，但是引发了许多反对意见，后续发展值得观察。

该法案试图通过多种方式来实现这一目标。最重要的是，CRA将要求市场在设计、构建、发行和维护软件时对安全性采用行业良好实践。在最基本的层面上，CRA正式确定了ASF现行的基本政策：管理您的错误，接受、分流并修复安全漏洞。这也是通过将其与良好的治理或实践相结合来实现的；例如，在适当的时候注册CVE（Common Vulnerability and Exposures常见漏洞和风险）、编写发行版说明和进行适当的版本管理（平心而论，其中一些我们应该进一步正规化和改进）。

译者注：ASF 现行的基本政策https://www.apache.org/security/committers.html

CRA还将试图确保欧洲市场上的所有软件都能达到某种最低的安全级别，具体做法是在CE符合性声明中进行相当简单的自我认证。或者，对于更关键的软件，如防火墙或安全加密密钥飞地，由外部、受监管的指定机构进行实际的"真正"认证和审计。CRA还将定义一系列流程，以监控市场的合规性。

*“CE”标志是一种产品安全认证标志（即只限于产品不危及人类、动物和货品的安全方面的基本安全要求，而不是一般质量要求），被视为制造商打开并进入欧洲市场的护照。CE 代表欧洲统一（CONFORMITE EUROP-EENNE）。
* 安全加密密钥飞地：是指硬件的处理器和内存的受保护部分。

欧盟政策制定者认识到，这些 "行业最佳实践" 还没有得到很好的定义（在整个行业内，ASF的安全实践是例外，而不是一体适用的规则）--许多CRA都依赖于国际标准组织来制定标准，人们可以用这些标准来审核自己的项目（自我认证），或者外部审核人员也可以使用这些标准。此外，人们还期望重大漏洞能得到特殊处理，并尽早报告。稍后再详述。

对开源的影响

如果你关注过各种博客和公开信，开源基金会一直在关注如何帮助完善CRA的现有措辞，使开源软件获得 "豁免"；也就是说，只有当代码离开了开源公域（译者注：Commons亦可翻译为公共资源）时，CRA才适用；然后继续适用于整个商业供应链。同时，当某些东西（如安全修复）再次进入公域时，《CRA-网络韧性法案》也不再适用。

博客：https://blog.opensource.org/what-is-the-cyber-resil-ience-act-and-why-its-important-for-open-source/
公开信：https://blog.opensource.org/the-ultimate-list-of-reactions-to-the-cyber-resilience-act/

总的来说，这些开源基金会或是社区的努力并不成功。《CRA-网络韧性法案》历次迭代的文件版本都有很大变化，但不是围绕着以上所述开源基金会或是社区关切的具体政策问题。为了了解原因，ASF的代表（连同OpenSSL）于7月7日直接与欧盟进行了对话，这是我们第一次真正能够与立法者进行有意义的互动。

从这次谈话中，我们了解到，政策制定者非常清楚，开源对IT行业至关重要，无论是对"生产"还是创新都是如此。正因为如此，他们希望避免杀鸡取卵。

译者注：政策制定者非常清楚
https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-impact-assessment

另一方面，欧盟立法者也意识到，开源通常占典型欧洲中小企业（SME）运营或获得许可的软件堆栈的 95% 或更多。而中小型企业作为将其推向市场的一方，要对整个软件栈负责。

据我们了解，政策制定者认为这些流程改进（和（自我）认证）的成本很高；大约会增加25%的管理费用。这是基于最近在医疗领域引入的类似法规和CRA影响评估（任何欧盟法律提案都需要将其可能产生的经济影响记录在案）。

因此，从中小型企业的整个堆栈（即95%的开源代码和5%的私家秘方）来看，对于大多数欧洲中小型企业来说，在全部100%的代码上额外付出的努力将是其工程努力的数倍，因此是不可行的。而欧盟的想法是，认证他们在开源堆栈基础上构建的5%或10%的代码要容易得多。

因此，政策制定者[1]向ASF明确表示，他们打算将CRA适用于开源基金会。目前，开放源代码的例外情况要么是纯粹的业余爱好者，要么是不在现实生活中使用的代码，要么是诸如镜像和软件包仓库（如 NPM 或 Maven Central）之类的东西。他们的做法是，如果软件在商业环境中的任何地方使用，就推定其具有商业意图。

[1] i.e. the people at the European Commission (DG-Connect) and the Rapporteurs -- the people at the European Parliament)

欧盟流程和 CRA 的现状

欧盟的一项立法通常由欧盟委员会起草（该委员会还负责准备“影响研究”等工作）。然后在议会进行讨论。讨论一般在较小的委员会中进行。这些委员会编写报告，最终立法提交议会全体会议表决[2]。

CRA的主要委员会是LIBE、IMCO和ITRE。第一个委员会是公民自由、司法和内政委员会（LIBE），负责讨论 "言论自由 "等问题，但该委员会拒绝提交报告。接下来，内部市场和消费者保护委员会（IMCO）研究了什么对消费者和内部市场是重要的。该委员会编写了一份报告，并提交给了工业、研究和能源委员会（ITRE）。

此后，工业、研究和能源委员会（ITRE）编制了一份协商一致的文件，预计将于20230717这一周进行公开讨论，并获得委员会的最终批准（在获得同意的情况下，委员会一般不进行表决）。

> 译者注：20230717这一周进行公开讨论
> https://www.europarl.europa.eu/committees/en/itre/home/highlights

一旦这项工作完成，提案将提交欧洲议会表决。根据当时的争议或共识程度，可能会、也可能不会进行讨论和自由表决。

> 译者注：工作完成
> https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-european-cyber-resilience-act

与此同时，欧盟的第三方--即欧盟理事会--也在准备其版本的法案。主要由各国的相关部长从本国的角度进行审议。然后，三个版本（欧盟委员会、议会和理事会）将在 "三方合议庭"（Trialogues）中进行闭门讨论，最后产生成为法律的最终版本。

法案推动的现状

目前，据说立法过程中的所有各方都已达成了大致的共识--其中有两方与ASF分享了他们的

[2] See https://www.consilium.europa.eu/en/council-eu/decision-making/ordinary-legislative-procedure/ for the details.

观点，即不存在争议。此外，各种共识文件的副本也已泄露--因此我们知道它们之间的差距并不大，现在我们也可以开始对它们进行分析了。

CRA给行业带来的问题

目前的定义[3]规定，《反垄断法》适用于ASF、及其所有（志愿）开发人员以及我们的所有产出。而且，根据ASF与政策制定者的会谈了解，这是有意为之。

对CRA的忧虑有很多，但对 ASF社区来说，以下几个问题可能是最重要的。

公域的概念与商业市场并无区别，它是一种全押模式：第一个问题是，《反垄断法》采取的是全有或全无的二分法。要么加入，要么退出。当你加入时，对你适用的基本上就是需要适用于出售给消费者的全套商业产品的内容。

虽然开放源码可能与此相近（如 Apache Netbeans 或 Apache Zeppelin，尽管没有实际商业产品出售），但开放源码一般不属于商业环境。相反，它可以作为共享知识或公共资源来管理。就像学术论文或参考蓝图一样。CRA并不承认这一点--因此，CRA完全适用于开源软件"（而不是仅仅适用CRA中在这种情况下可能有意义的要素--如良好的漏洞处理、版本控制和“软件物料清单-SBOM”）。

除非开源项目具有 "完全分散的开发模式"，否则CRA将对其进行监管。然而，"公司" 雇员拥有贡献提交（commit）权的项目将不会被豁免（无论上游开源合作是否与其雇主的商业产品有任何或是毫无关系）。有些项目，如古老的OpenSSL项目，其模式甚至更为复杂。

> 译者注：OpenSSL项目，其模式甚至更为复杂
> https://www.openssl.org/blog/blog/2023/07/17/who-writes-openssl/

这颠覆了开源的双赢原则。如果禁止企业维护者，企业可能会放弃让其员工维护项目，从而损害开源创新生态系统，具有讽刺意味的是，这将破坏其韧性及其对经济/增长的巨大推动作用（根据欧盟影响评估，每年90亿欧元）。

这也让人很难看出ASF社区中有谁会去做ASF可能被要求需要做的额外的（自我）认证工作。

[3] both in the Council and in the ITRE consensus documents (that includes IMCO input)

[4] This is the section of the Act that explains and sets the context for the remainder of the document. It is here that the intent is documented.

这样做的净效果实际上相当广泛。举一个"序言[4]，10a"中的例子（这样的例子还有很多）：**同样，如果自由和开源项目的主要贡献者是受雇于商业实体的开发人员，而且这些开发人员或雇主可以控制代码库中接受哪些修改，则该项目一般应被视为具有商业性质。**

在这里，这些贡献者与商业雇主之间缺乏交易关系的联结是个问题。例如，开发者可以是受雇于商业航空公司（即商业实体）的飞行员，利用业余时间为开源做出贡献：这部分政策将使这种贡献具有"商业性"。此外，在ASF，主要贡献者（提交者）当然可以对进入代码库的内容进行一定程度的控制[5]。

译者注：意即与开源没有半毛钱关系的雇主航空公司也将遭受池鱼之殃，而被列入监管范围内。

更糟糕的是，受影响最严重的开源组织类型也正是那些如今往往拥有非常成熟的安全流程的组织，它们负责任地分流、修复和披露漏洞，并提供与之相匹配的CVE（常见漏洞和风险）。一般来说，CRA需要在下游，即将产品投放到市场上的公司中推动重大改进。而现在却有可能出现相反的情况。

CRA影响了完全由志愿者领导和驱动的项目（如ASF），在这些独立自主的ASF项目中，没有任何公司能对产品的操作和发布有任何影响。而CRA将对任何商业实体的员工拥有贡献提交（Commit）权的项目都会受到影响。

这就带来了一个问题：无论是商业公司还是开源项目，都需要对哪些提交者可以修改代码、接受哪些资助以及接受哪些补丁等问题更加谨慎。

在CRA认证中，有一个很强的假设，即模块的（自我）认证是 "传递性" 的；也就是说，如果你用经过认证的模块构建了一些东西，你只需要认证你所做的"额外"的一些事情。不幸的是，这在一般情况下是不正确的；认证通常在很大程度上是要表明你（作为最终承担责任的组织）是如何确保所交付的东西适合你在客户的特定环境下交付的目的。开源组织在自我认证其构建的软件模块时，并无法提供“上游”信息。

认证的核心是确保所发布的信息对其预期目的具有适当的安全性。具体地说，就是在设计时就考虑到安全问题，规划出威胁行为者、载体和风险。然后根据风险做出合理的工程妥协。

遗憾的是，在开源领域，我们往往不知道我们的软件会被如何使用。而且，正如我们在过去十年中学到的（困而知之），对于我们良好治理共享资源来说，关键是我们不能在许可证中（译

[5] A much better version would be:

者注：对如何使用开源软件）进行歧视或限制（事实上，这也是开源定义的一部分）。

> 译者注：开源定义Open Source Definition 是OSI制定关于开源许可协议的10条基本原则。违反这些原则的许可协议，不得自称为 ”开源” 许可协议。开源定义：
> https://zh.wikipedia.org/zh-cn/%E5%BC%80%E6%BA%90%E5%AE%9A%E4%B9%89

有些义务几乎是不可能履行的：例如，有一项义务是 "提供没有已知可利用漏洞的产品"。这几乎是一个不可能设定的标准；尤其是开源软件的作者既不知道也无法控制他们的代码是如何被整合到下游的。

下一个问题与标准有关。CRA提到了大量 "待编写 "的国际标准（一般认为由CEN-CENELEC制定）。一般来说，IT行业，尤其是开源，在与这些标准机构合作方面并没有很好的记录（也包含了ASF），部分原因是几乎所有关键的互联网标准都由IETF和W3C维护。事实上，这些标准组织的章程不允许开源组织以有意义的方式成为其成员的情况并不少见。

> 译者注：不允许开源组织以有意义的方式成为其成员
> https://blog.opensource.org/another-issue-with-the-cyber-resi-lience-act-european-standards-bodies-are-inaccessible-to-open-source-projects/

CRA要求在漏洞修复前，以小时为单位的时限内向ENISA（欧盟机构）披露严重的未修补漏洞和被利用漏洞。这与行业最佳实践--负责任地披露修复和（变通的）解决办法--背道而驰。

而且，这种过早的报道不仅会分散发布修复信息的注意力，对于国际社会来说，还很容易触犯其他国家坚持要相同信息的规定，或者更糟糕的是，禁止分享此类信息。这就破坏了开源所依赖的公平公正的报告的文化核心。

而且，只有当这些信息被广泛共享时，才会对ENISA有用--因此，各组织理应选择谨慎、全球"公平"的方案，采取简单易行的方法：确保永远不会听说这些问题。或者，反其道而行之，在（第一个）报告截止日期结束之前，即在问题得到解决之前，将问题公之于众。

> 译者注：意即在问题解决前，不对外公布；或是一有问题，立即全球公布。而不是优先将问题只通知某些特定机构，如欧盟的ENISA。

因此，这又是一个例子，说明CRA虽然用心良苦，但最终可能适得其反。

一个有效的CRA

纵观欧洲目前的IT行业，我们可以发现，造成IT行业安全状况不佳的根本原因通常并不是开源（尤其是来自ASF这样的组织）。事实上恰恰相反。

与此相反，欧洲的大多数中小型企业很少更新他们所依赖的系统，通常也不擅长处理安全问题报告。而ASF的（定期）更新为他们带来了更多的（重新）认证工作，可能会使他们更慢地接受我们的更新和安全修复。

不过，CRA中也有很多可行的方法，而且我们知道这些方法很可能会有效；在开源组织（如ASF）层面也是如此。

事实上，我们今天已经做到了大部分，例如对漏洞报告进行良好的分流、负责任的披露、注册CVE（常见漏洞和风险）以及谨慎使用版本号。在此基础上，我们还实行了良好的治理，各项目都要向董事会报告，偶尔也会有项目在时机成熟时被转移到阁楼上（译者注：束之高阁，意即项目进入退役或退休状态）。

问题更多的在于，CRA还提出了一系列要求，这些要求要么威胁到开源贡献或我们的公有（或共享）领域非常脆弱的"双赢"局面，要么违背行业良好实践，要么根本不可能实现，也就是说，它试图将开源公有领域与商业领域等同对待。

事实上，美国似乎已经意识到了这一点，并正在与美国国家标准与技术研究院（NIST）合作，与业界一起记录这些现有的良好实践。

在某种程度上，美国似乎更接近于历史上由工程师和个人主导的ACME程序，该程序产生了锅炉规范；而欧盟似乎更倾向于询问制造商，而不是专家。

互联网如此绕开这样的问题

"互联网将审查制度这一运转良好的机制（就如同房间里的一头大象确实存在）视为故障，并绕开它"（约翰-佩里-巴洛）。

> 译者注：房间里还有一头大象：意指 “一个问题因太过于庞大或麻烦，导致没有人愿意去碰”

上世纪90年代，当美国试图对加密软件进行监管时，我们看到了这一机制的作用。只有“达到出口规范要求” 的加密软件技术才能离开美国。

这导致大量加密行业和人员从物理上和法律上离开美国，并将该行业从美国转移到欧洲。在那里，公司只需将其代码输入美国，或从欧洲将其运往世界各地，不受美国出口管理局（BXA: The Bureau of Export Administration）规则的限制。二十多年后，这种情况才得以正常化（我们在ASF中仍然可以看到这种情况的残余）。

因此，ASF还需要考虑到我们的社区可能会因CRA而分裂的风险。尤其是当我们散布在欧洲各国的ASF项目社区不能调动足够的能力和实力来在ASF项目上实施CRA。

译者注：ASF中仍然可以看到这种情况的残余https://www.apache.org/licenses/exports/

行动时间表

2023年7月17日这一周将举行工业、研究和能源委员会（ITRE）投票。这是一个向欧洲议会成员建议如何投票的议会委员会。投票结束后，2023年夏季休会后可能将开始三方讨论（Trialogues：欧洲议会、欧盟理事会、欧盟委员会）。如果三巨头达成共识（目前看来如此），这一进程最早可能在12月结束。

因此，在很短的时间内，人们可以联系工业、研究和环境部的欧洲议会议员。一般来说，如果这些信息是礼貌性的，由具有一定政治或经济地位的一方（如中小型企业组织的首席执行官）发送，并且符合当地的环境，如用当地语言发送给本国的议员，并注意他们所代表的政党的政治立场，则会有所帮助。

由于对开源的监管是有意为之，而且《CRA：网络韧性法案》中也有很多具备常识性的良好（开源）实践：目前的期望值是，我们（开源社区）已经有所斩获并且已经过了要求全面例外的阶段。

译者注：工业、研究和环境部的欧洲议会议员https://www.europarl.europa.eu/committees/en/itre/home/members

ASF将专注于欧盟理事会版本（因为其文本通常在三方讨论中 "胜出"，而且现在比ITRE的共识文本更好一些）。为此，我们需要您的帮助：特别是，如果您能帮助我们让贵国较具规模的中小企业高管参与进来，并愿意在国家层面解释CRA将造成的负面影响（请联系ASF公共事务副总裁；dirkx@apache@org）。

译者注：最后的几个段落的诉求看起来比较隐晦，其实就是说 ”开源尚未成功，同志仍需努力”！

原文链接：https://news.apache.org/foundation/entry/save-open-source-the-impending-tragedy-of-the-cyber-resilience-act

面对法律，开源应为安全负什么责任

卫剑钒

《大教堂与集市》译者，《安全协议分析与设计》作者，国际信息系统安全认证专家（CISSP），中国金融学会金融科技专委会委员。

本文主要考虑两个法律，我国的《网络安全法》[1]（以下简称“网安法”）和欧盟的《网络韧性法案》（以下简称“CRA”，欧盟议会修正案版本[2]），另外，还会涉及我国的《网络产品安全漏洞管理规定》[3]（以下简称“漏洞管理规定”）。

本文主要就以下几个问题做讨论：

[问题1]在开源产生之日起就有‘开源开发者免责’能否、在何种程度上行得通？

[问题2]开源项目是否要适用网络安全相关法律？特别是发现安全漏洞是否要履行上报义务？

[问题3]有涉欧业务的非欧盟企业发现漏洞先上报欧盟还是本国，本国不允许对外披露漏洞怎么办？

[问题4]开源基金会应当承担什么样的责任？

一、开源到底要不要负责任？

了解过开源许可证的人都知道，几乎所有的开源许可证，都明明白白说了“不负责任”。

比如最常见的MIT协议，是这么说的：

本软件系“按原样”提供，不包含任何形式的明示或默示保证，包括但不限于适销性、特定目的适用性及不侵权的保证。在任何情况下，无论是在合同、侵权或其他案件中，作者或版权持有人均不对因本软件、或因本软件的使用或其他利用而引起的、引发的或与之相关的任何权利主张、损害赔偿或其他责任承担责任。[4]

---

[1]《中华人民共和国网络安全法》请见：https://flk.npc.gov.cn/detail2.html?MmM5MDlmZGQ2NzhiZjE3OTAxNjc4YmY4Mjc2ZjA5M2Q%3D

[2]该法案尚未生效，欧盟议会于2023年7月26日对CRA法案提案的修正版本请见：https://www.europarl.europa.eu/doceo/document/A-9-2023-0253_EN.html

[3]《网络产品安全漏洞管理规定》请见：https://www.gov.cn/zhengce/zhengceku/2021-07/14/content_5624965.htm

开源项目作者是不是认为这样，就不会有任何外部麻烦了呢？

未必。

因为所有许可证，都得遵从法律，并不能突破法律的约束。如果有不一致的地方，以法律为准。

通常而言，开源项目的产出是软硬件，我们看看法律对软硬件规定了哪些安全要求。

二、法律对软硬件的安全要求

在网安法中，最相关的是第二十二条：

第二十二条 网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

在网安法中，最相关的是第二十二条：

本法规规定了（a）具有数字元素的产品在市场上的销售规则，以确保此类产品的网络安全；（b）具有数字元素的产品的设计、开发和生产的基本要求，以及与这些产品相关的经济运营者在网络安全方面的义务；（c）具有数字元素的产品的制造商关于漏洞处理流程的基本要求，以确保产品在整个生命周期内的网络安全，以及经济运营者对这些流程的义务；（d）对上述规则和要求进行市场监控、监督和执行的规则。

当然，在其后的条款中，有着更为详细和具体的安全规定与要求。

仔细阅读，可以看出，这些法律法规，主要是说网络产品的制造者、提供者这些主体，应该保证产品是安全的，并且在发现漏洞后，要及时报告和处置。

那么，开源项目的产出是不是“网络产品”，是不是“具有数字元素的产品”呢？

尤其是，作为一种最常见的情况，那些放在GitHub上的开源项目的产出，是不是法律所关注的产品？

这就需要细究对“产品”的定义。

[4] MIT原文请见https://opensource.org/licenses/MIT，译文请参考《从MIT协议谈契约精神》：https://mp.weixin.qq.com/s/GGf0pMaIZVb6ykBBWdjNlg，以及“源译识”MIT译文审定稿：https://gitee.com/OpenAtomFoundation/legal-license-translation

这就需要细究对“产品”的定义。

然而，这并不容易。

三、令人头疼的关于“产品”的定义

网安法并没有给出“网络产品”的定义，而是直接使用。

那就很难直接回答“开源项目产出”是不是“产品”了，毕竟在《现代汉语词典》[5]中，**“产品”是“生产出来的物品”，而“生产”是指“人们使用工具来创造各种生产资料和生活资料”**，如此而言，我在家里做一个自用的小桌子，也是《现代汉语词典》所认为的“产品”。

但在大多数人的直觉感受上，“产品”应该是制作出来销售的东西。

我在《民法典》中，也没有找到对“产品”的定义，但在我国的《产品质量法》[6]中，发现了对“产品”的定义，它的第二条中，明确写道：

本法所称产品是指经过加工、制作，用于销售的产品。

虽然我不知道《产品质量法》中对产品的定义能否用在《网安法》中，但我认为大体上可以类比，在民法典和网安法中，也确实都提到了产品的“销售”，也都没有提及不用于销售的产品如何规范，所以，**我认为，网安法中的产品，应该不是泛指所有制作出来的物品，而更多是说指商业活动中的产品。**

现在看看CRA。

CRA全文都是在描述对“具有数字元素的产品”（product with digital elements）的要求，并在第3条给出了定义：

‘product with digital elements’ means any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately;

翻译：“具有数字元素的产品”是指任何软件或硬件产品及其远程数据处理解决方案，包括单独投放市场的软件或硬件组件；

我们看到，对“XX产品”的定义为“是指blablabla的产品”，那事实上就是没有定义“产品”。

但CRA在第二条明确说明了适用范围：

[5] 《现代汉语词典》(第 7 版)

[6] 《中华人民共和国产品质量法》(http://www.npc.gov.cn/zgrdw/npc/xinwen/2019-01/07/content_2070255.htm)

本法规适用于市场上提供的具有数字元素的产品，这些产品可以与设备或网络直接或间接数据连接。

这里明确了一点，但还是不够，因为“市场”未必一定是商业的，**“市场”是需求和供给相遇并通过某种机制达成交换的场所**，完全可以把GitHub认为是一个代码市场，程序员和用户在这里实现需求和供给的交换：有人需要代码，有人提供代码。

幸好，CRA在第3条中对“在市场上提供”也做了定义：

“在市场上提供”是指在商业活动中，无论是有偿还是免费，将带有数字元素的产品提供给联盟市场以供分发或使用。

这样，疑惑就完全解开了。法律中所说的“网络产品”、“具有数字元素的产品”，我认为，都明示或暗示了这样的条件：

所谓产品，是指用于商业活动的产品。

所以，对于那些并不参与任何商业活动，仅仅是放在GitHub或是类似的代码托管平台上的开源项目，法律是不管的。

但，开源项目一旦涉及商业活动，相关主体就要受到约束。

这就是开源商业化的代价。

四、哪些主体应该受到约束

在《网安法》中，最主要的受到约束的两个主体是**“网络运营者”和“网络产品、服务的提供者”。**

在网安法的附则中，对“网络运营者”有定义，“是指网络的所有者、管理者和网络服务提供者。”网安法对“提供者”没有定义，但这相对容易理解，提供者应该是指产品的生产者、经销者、集成者等。

在CRA中，涉及的主体主要是“**经济运营者**”，主要是指制造商、进口商、分销商等，每个主体在CRA第3条中有定义。

这些主体的义务，正如本文前面所提到的，在法律条文中有明确而详细的规定。

综上，开源项目只有涉及商业活动，其相关主体才受到法律约束。

这就是对【问题1】的回答。

然而，现实要更复杂一点，什么是涉及商业活动?

举个例子，一个开源软件，同时提供社区版和企业版，那么其社区版是否涉及商业活动?

五、如何判别开源涉及商业活动?

网安法没有明确提及这些，但CRA有说。CRA不仅说了，而且把这个说得很清楚。在其序言部分的第10条中，明确说道：

(10)只有在商业活动过程中在市场上提供的自由和开源软件才应受本法规管辖。自由开源产品是否作为商业活动的一部分提供，应根据每个产品进行评估，同时考虑免费开源产品的开发模式和供应阶段。

(10a)例如，**在完全去中心化的开发模式中，没有任何一个商业实体对项目代码库中接受的内容进行控制，这应该被视为该产品是在非商业环境中开发的。**另一方面，如果自由和开源软件是由单个组织或不对等社区开发的，并且单个组织通过对其使用（与商业有关联）产生了收入，则应将其视为商业活动。同样，如果自由和开源项目的主要贡献者是商业实体雇用的开发人员，并且当这些开发人员或雇主可以控制代码库中接受哪些修改时，该项目通常应被视为商业性质。

(10b)在供应阶段，自由和开源软件的商业活动可不只是对产品收费，**对技术支持收费也是商业活动，除非该收费只是为了收回实际成本；自由和开源软件的制造商提供一个软件平台并通过其他服务收费也是商业活动；出于除专门提高软件的安全性、兼容性或互操作性以外其他原因而使用个人数据也是商业活动；**不以营利为目的接受捐赠不应被视为商业活动，除非此类捐赠是由商业实体提供的并且具有经常性。

(10c) 单独为自由和开源项目做出贡献的开发人员不应承担本法规规定的义务。

(10d)仅仅在开放式代码库上提供对自由和开源软件的托管，该行为并不构成在市场上提供具有数字元素的产品。因此，大多数软件包管理器、代码托管和协作平台不应被视为本法规含义内的分销商。

(10e)……如果产品制造商发现组件（包括免费和开源组件）中存在漏洞，则应通知该组件的开发人员，解决并修复该漏洞，并且在适用的情况下，为开发人员提供应用的安全修复。一旦制造商将产品投放市场，就应负责确保在整个支持期内处理产品中漏洞，包括其中集成的自由和开源组件。

以上几条，足以解决绝大多数关于开源项目是否涉及商业活动的困惑了。比如，按照以上定义，GitHub不是市场，GitHub公司也不是分销商，无需承担CRA中所述的分销商义务。再比如，谷歌提供了Andriod平台但通过服务收费，属于受管辖范围；RedHat收取技术支持费，属于受管

辖范围；XX社区版有助于XX企业版的销售，所以XX社区版被认定为涉及商业活动。**当然，这个认定，需要“根据每个产品进行评估”。**

如果仅仅是对开源项目作出个人贡献，不适用CRA。没有任何商业化行为的开源项目，也不受管束。

之所以这样做，原因很简单，也很符合常识，在序言第9a里面说，这是“为了促进自由和开源软件的开发和应用”。

多说一句，如果你是用别人的非商业化开源软件搞自己的商业化，别人不用负责，但你要为那个开源软件负责任。

毕竟是你挣钱嘛。

在我国的法律上，以上这些虽然没有明说，但事实上也是按照这个原则执行的。

也就是说，通过一事一议的鉴别，如果一个开源项目涉及商业活动，相关主体就要受法律约束，包括发现漏洞后的上报。

以上就是对[问题2]的回答。

六、发现漏洞后如何报告?

这并不是个问题，因为怎么报、报给谁，法律或相关规定都有写得很明确，没有歧义。比如在我国的《网络产品安全漏洞管理规定》中，第七条说明了产品提供者的义务：

第七条 网络产品提供者应当履行下列网络产品安全漏洞管理义务，确保其产品安全漏洞得到及时修补和合理发布，并指导支持产品用户采取防范措施：

（一）发现或者获知所提供网络产品存在安全漏洞后，应当立即采取措施并组织对安全漏洞进行验证，评估安全漏洞的危害程度和影响范围；对属于其上游产品或者组件存在的安全漏洞，应当立即通知相关产品提供者。

（二）应当在2日内向工业和信息化部网络安全威胁和漏洞信息共享平台报送相关漏洞信息。报送内容应当包括存在网络产品安全漏洞的产品名称、型号、版本以及漏洞的技术特点、危害和影响范围等。

（三）应当及时组织对网络产品安全漏洞进行修补，对于需要产品用户（含下游厂商）采取软件、固件升级等

措施的，应当及时将网络产品安全漏洞风险及修补方式告知可能受影响的产品用户，并提供必要的技术支持。

……

CRA中则在第十一条的1a中说明了制造商的义务：

（a）**在制造商意识到存在被积极利用的漏洞后的 24 小时内发出早期警告**，不得无故拖延，包括是否有任何已知的纠正措施或建议的风险缓解措施可用；

（b）**制造商应在意识到存在被积极利用的漏洞后 72 小时内发出漏洞通知**，不得无故拖延，如果适用，应更新(a)中的信息，包括采取的任何纠正措施或缓解措施，并指出漏洞的危害程度，包括其严重性和影响；

（c）**当纠正措施或缓解措施可用时，或当(b)发出后一个月内，应提交漏洞最终报告，**至少应包括以下内容：(1) 对漏洞的描述，包括其严重性和影响；(2) 如果有的话，给出已利用或正在利用漏洞的行为者的信息；(3) 为修复漏洞而提供的安全更新或其他纠正措施的详细信息。

其中，所谓“被积极利用的漏洞”，是指“有可靠证据表明攻击者在未经系统所有者许可的情况下在系统上执行了恶意代码的漏洞”。

对于有涉欧业务的中国企业，要注意学习CRA，按照如上要求及时报告，报告对象是ENISA（欧盟网络安全局）。

有人说，“对于有涉欧业务的中国企业，发现漏洞先上报欧盟还是我国，我国不允许对外披露漏洞怎么办？”这看似是一个难题，实则不然，处理起来也很简单。

第一：对于我国，要在2日内报。对于欧盟，要在24小时、72小时内报。

第二：并不冲突，我国并没有说不让对外批露，漏洞管理规定只是说在第九条里说，“从事网络产品安全漏洞发现、收集的组织或者个人”“不得将未公开的网络产品安全漏洞信息向网络产品提供者之外的境外组织或者个人提供。”

这里的约束主体是专门从事漏洞发现和收集的组织和个人，而非“网络产品提供者”。在对提供者的要求中（见第七条），没有类似的约束。

也就是说，从漏洞管理规定上看，对于未公开的漏洞，发现者可以告诉提供者，但未公开前不能告诉提供者之外的境外组织和个人；有涉欧业务的产品提供者，一旦发现漏洞，不管是否已公开，没有说不能报告ENISA。

因为，发现者可能远早于制造商知道漏洞，如果告诉境外某些组织或个人可能给敌对方带来极大便利。而制造商知道漏洞后，必须第一时间告诉监管机构（不管境内境外），并抓紧给出修复或缓解方案，禁止制造商报告境外监管机构意义不大，除非我们不信任ENISA。

在这方面，这两个法规并不冲突。

这是对【问题3】的回答。

七、法律对基金会的约束是什么？

对这个问题，也要一事一议，要具体看一下某基金会的性质。

我们知道，基金会旗下有很多开源项目，基金会为其提供组织、法律和资金上的支持，那么，能否认为基金会就是开源软件的制造商或分销商？

对此，有人很焦虑，觉得一旦落入什么商，基金会可能无法承担起如此沉重的安全义务。

其实，我觉得并不难，虽然CRA并没有具体说基金会算什么性质，但在序言第10条中其实已经说明了：

如果“没有任何一个商业实体对项目代码库中接受的内容进行控制，这应该被视为该产品是在非商业环境中开发的。”

“不以营利为目的接受捐赠不应被视为商业活动，除非此类捐赠是由商业实体提供的并且具有经常性。”

一个基金会的项目，是不是有商业实体在对项目进行控制，基金会是不是以营利为目的接受捐赠，若涉及具体的案子，相信不难做出调查和判断。

比如ASF（Apache软件基金会），其宗旨之一就是：

“项目独立于任何公司或组织的影响”

如果ASF真的是这样做的，那就显然不在CRA管束范围之内。

但有的基金会显然不是这样，这里就不点名了。

这是对【问题4】的回答。

以CRA为视角看开源项目的《网络安全法》适用

陶冶

国浩律师（南京）事务所 律师

南京市律协知识产权法律专业委员会、数字经济法律专业委员会委员

taoye@grandall.com.cn

摘要

开源项目是否受到《网络安全法》调整一直备受关注。从《网络安全法》的基本定位、具体规范，结合欧盟立法例来看，开源项目应当落入《网络安全法》的调整范围。开源软件的直接对外提供者，以及开源代码仓库或某一分支的控制者应当承担网络安全义务。但承担义务并不意味着网络安全问题上的无限责任，其义务仍以《网络安全法》的明文规定为限。同时，开源项目的普通贡献者因不构成《网络安全法》上的提供者，并不在前述义务主体之列。

关键词： 网络安全法，开源，CRA

一、引言

《网络安全法》是我国网络空间治理的“基本法”[1]，其以“保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展”为根本立法目的，对在境内建设、运营、维护和使用网络的主体做出了一系列规范。对于开源开发者来说，最为重要的条款当属《网络安全法》第22条第1、2款的规定。

前述2款为“网络产品的提供者”设定了以下4项义务：第一，网络产品、服务应当符合相关国家标准的强制性要求；第二，网络产品、服务的提供者不得设置恶意程序；第三，发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有

[1] 参见中国网信网：《<网络安全法>的立法定位、立法框架和制度设计》，http://www.cac.gov.cn/2016-11/07/c_1119866606.htm,最后访问时间：2023年11月19日。

关主管部门报告；第四，网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。

但由于《网络安全法》基础性法律的定位，不可避免会出现法律表述上的原则性[2]，因此对于开源软件的开发者是否负有《网络安全法》上的义务这一问题，仍有模糊之处，有待进一步的澄清。

鉴于网络安全问题的国际性，以及《网络安全法》立法时主要制度与国外通行做法保持一致的基本理念[3]，域外立法例对理解《网络安全法》的具体制度有着重要的借鉴作用。因此，本文拟结合以《网络韧性法案（草案）》（Cyber Resilience Act，以下简称CRA）为代表的欧盟立法例，通过比较法的视角对这一问题展开研究。

二、什么是“网络产品”

《网络安全法》并未对何为“网络产品”做出明确规定，但理解“网络产品”这一概念的定义，对明确“网络产品的提供者”这一义务主体至关重要。

对于这一概念的争议主要集中在两个方面，第一，免费提供的开源软件，是否构成产品；第二，对于不直接面向用户的中间件以及系统软件，是否属于“网络产品”。本文围绕前述两个问题展开详述。

（一）“网络产品”应当包含免费提供的开源软件

从文意上理解，“产品”二字并不能与“收费”直接挂钩。根据《产品质量法》第二条第二款的规定：“本法所称产品是指经过加工、制作，用于销售的产品”。《产品质量法》该款看似循环定义，其实质为根据《产品质量法》规范的范围对“产品”概念在该法范围内进行限缩，即仅限于“用于销售”的产品。通过该限缩性规定可以看出的一个基本逻辑是，“产品”这一概念本身即包含“用于销售”和“非用于销售”两种。也就是说，除非有明文规定进行限缩，“网络产品”这一概念不能排除免费提供的开源软件。

[2] 前引1。

[3] 参见全国人大常委会法制工作委员会副主任 郎胜：《关于《中华人民共和国网络安全法（草案）》的说明》，2015年6月24日。

义，其实质为根据《产品质量法》规范的范围对“产品”概念在该法范围内进行限缩，即仅限于“用于销售”的产品。通过该限缩性规定可以看出的一个基本逻辑是，“产品”这一概念本身即包含“用于销售”和“非用于销售”两种。也就是说，除非有明文规定进行限缩，“网络产品”这一概念不能排除免费提供的开源软件。

欧盟的网络安全立法例中，2019年的《欧盟网络安全法案》（Cybersecurity Act，REGULATION (EU) 2019/881）中，将ICT产品（ICT Product）定义为：“网络或信息系统的一个要素或一组要素。”（‘ICT product’ means an element or a group of elements of a network or information system）[4]，在对“产品”进行定义时也未区分收费亦或是免费。

在CRA中，虽然目前欧洲议会以及欧盟理事会的提案的措辞略有不同，但大意基本一致，以欧洲议会2023年7月提案为例（本文以下部分除非特别提及，对CRA的引用均以欧洲议会版本为准），其对“带有数字元素的产品”（product with digital elements）的定义为：“任何软件或硬件产品以及其远程数据处理的解决方案，包括单独投入市场的软件或硬件组件。”（any softwareor hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately）[5]，仅从该条看来，似乎是对软件或硬件组件做了特别规定，只有投入市场（be placed on the market separately）方才构成“产品”或被拟制为“产品”，而非组件的软硬件，无论是否投入市场均构成“产品”。但这样的单独限缩并没有任何立法目的上的支撑，在逻辑上也显得不甚协调，因此并不能急于得出结论。对CRA文本进一步分析可以发现，CRA第3条第（18）款进一步将“制造者”（manufacturer）定义为：“任何自然人或法人，他们开发或制造带有数字元素的产品，或者让其他人设计、开发或制造这类产品，并以其名字或商标将这些产品投放市场，无论是出于收费、商业化还是免费的目的。”（anynatural or legal person who develops or manufactures products with digital elements or has products with digital elements designed, developed or manufactured, and markets them under his or her name or trademark, whether for payment, monetisation or free of charge）[6]，即同一主体必须同时满足制造了“带有数字元素的产品”并且实施了“投放市场”的两种行为时方才构成CRA中规定的制造者，进而落入了CRA的规制范围。而在第3条第（23）款上则将“在市场上提供”（makingavailable on the market）定义为：“在商业活动过程中，为了在欧盟市场上的分销或使用而提供带有数字元素的产品，无论是作为有偿还是免费”[7]，结合前言（preamble）第（10）款的表述，前述一系列定

[4] REGULATION (EU) 2019/881, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0881&qid=1700381003823，last visited: 19 November 2023.

[5] AMENDMENTS BY THE EUROPEAN PARLIAMENT to the Commission proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 and Directive 2020/1828/EC (Cyber Resilience Act)，https://www.europarl.europa.eu/doceo/document/A-9-2023-0253_EN.html, last visited: 19 November 2023.

[6]前引5 [7]前引5

的目的在于将非以商业目的免费和开源软件排除在CRA的规制范围之外。基于这样的定义，如若“产品”一词当然包含“商业化”的前提的话，那么“制造者”定义中的制造“产品”+“投放市场”的表述则将构成循环定义，额外以“投放市场”对“制造者”概念进行限缩也就不再有任何意义，这种解释显然与CRA的体系相矛盾。因此，在CRA的语境下，构成“产品”也不以商业化为前提。

至于前文“带有数字元素的产品”定义中的“单独上市”，考虑到当前CRA仍未正式颁布，本文认为该定义应理解为“单独对外提供”，而非强调其在市场上进行的商业化投放。

因此，我国《网络安全法》中，一方面即没有像《产品质量法》中一样对产品一词直接进行限缩，另一方面也没有像CRA一样通过其他方式排除免费软件。结合“产品”一词的一般意思，《网络安全法》中的“网络产品”应当包含了免费提供的开源软件。

（二）“网络产品”应当包含中间件

首先，根据国家标准《信息安全技术网络产品和服务安全通用要求》（GB/T 39276—2020）的定义，网络产品的定义为：“作为网络组成部分以及实现网络功能的硬件、软件或系统,按照一定的规则和程序实现信息的收集、存储、传输、交换和处理。”该定义并未将网络产品限定为系统软件和应用软件。且实践中大量的网络安全漏洞就存在于中间件之中（如Log4j2漏洞），从立法目的上也无排除中间件的可能。

从欧盟立法例看，前述《欧盟网络安全法案》中ICT产品的定义显然包括中间件。CRA的定义中，则是专门强调了“组件”（components）也属于CRA的规制范围。

据此，结合国内标准以及域外立法里的有关定义，《网络安全法》中的“网络产品”应当被解释为：包括免费以及中间件在内的，一切作为网络组成部分以及实现网络功能的硬件、软件或系统。

三、“网络产品的提供者”的范围

在《网络安全法》中网络产品的定义明确后，还需进一步分析“提供者”的范围。此处的“提供”行为可分两种情形讨论，第一种情形为某一主体直接对外提供软件，如对外销售或以其名义提供副本，这种情况中的提供者下文中统称为名义提供人。另一种情形则为通过开源平台对外开放的情形。前者的名义提供人毋庸置疑属于提供者。但对于后者，每一个如此对外提供的开源软件

都至少涉及一个控制者（控制者可以是个人、组织或社区）和若干贡献者等多重主体。此时如何界定《网络安全法》语境下的“提供者”就显得至关重要。界定《网络安全法》语境下的“提供者”就显得至关重要。

本文认为，基于“法不强人所难”的基本法理，法律不应超出主体的能力范围去给某一主体设定义务，即只有可能履行《网络安全法》赋予的义务的主体方才可能构成《网络安全法》下的提供者。结合本文开头提到的四项义务，在通过开源平台开放软件的场景下，“提供者”至少应为某分支的控制者，即有权决定是否合并某些代码进入分支乃至决定是否删除该分支的主体方才可能构成该分支对应的网络产品的提供者，而仓库的控制者因权限更高，也应属于此处的提供者。但普通的贡献者因无权决定网络产品的具体特性、恶意程序的排除和加入以及是否继续维护等事项，并不会仅仅因其贡献的软件系开源软件而落入“提供者”范畴。

在CRA中，对“制造者”则是提供了更为明确的释义，将其限于“以其名字或商标将这些产品投放市场”的主体，即投入市场的名义人，这一定义因未包含了未采取任何商业行为的分支或者仓库控制者，其范围相较《网络安全法》更窄。

据此，我国《网络安全法》中的网络产品提供者即应当包括直接对外提供网络产品的名义人，也包括开源社区中某一具体分支的控制者或整个仓库的控制者。

四、结论

如前所述，无论是免费的开源项目亦或是收费软件，也无论其是应用软件、操作系统亦或是中间件，均落入了《网络安全法》的规制范围，而此类软件名义提供者，或是开源平台上某仓库或分支的控制者则需履行《网络安全法》上的有关义务。

但这不意味着无限的义务，也并不意味着会对开源生态造成毁灭性的打击。正如本文开篇所列明的产品提供者的四项义务，其中有强制性标准的贯标义务，有得知漏洞后的报告和采取措施的义务也有提供维护服务的义务，各项义务均有明确的范围以及期限，包括开源领域中常见的“ASIS”条款也有通过《网络安全法》第22条第2款后段进入公法领域的可能，本文限于篇幅无法一一展开。

对于开源参与者来说，了解和遵守《网络安全法》规定的义务边界至关重要，这不仅有助于他们更好地维护网络空间的安全和秩序，同时也能更有信心和明确性地参与到开源生态的建设和发展中。

开源人才观专栏介绍

1.专栏概述

随着科技的飞速发展，人类社会已进入数字化和信息化时代。数字经济的发展，给人才的观念和认知带来了重大的变化。在数字经济中，人才不再是被动的接受者和执行者，而是主动的创造者和贡献者。人才不再是封闭的个体和群体，而是开放的网络和社区。人才不再是稳定的资源和资产，而是动态的能力和价值。如何有效地培养、使用和激励这类人才，使其在数字经济时代发挥最大潜能，成为当前亟待解决的一个重要课题。

为了引领数字人才的发展，开放原子开源基金会提出了开源人才观的全新概念，作为数字人才发展的参考框架。这一框架旨在促使企业、组织和个体更好地适应数字经济的发展要求。

1）专栏的主要内容

《开源人才观专栏》立足于数字经济时代背景，聚焦开源人才这一主题，从多个维度出发，深入探究其培养、使用、评价和激励等方面的内容，旨在为相关领域的工作者和研究者提供有益的理论指导和支持，促使开源人才人才发展更好地适应快速变化的数字化环境。

专栏将从以下几个方面进行探讨，包括但不限于：

1.开源人才培养框架设计：专栏将深入研究开源人才的培养目标、要求和方法。通过对教育、企业和社会等多个层面的研究，提出创新性的培养策略，以培养具备开源精神、协作能力、技术实力和社会责任感的数字化专业人才。

2. 开源人才的使用和配置策略：专栏将聚焦于企业对开源人才的使用和管理。通过深入研究企业如何招聘、培养和激励开源人才，提供实用的建议，以确保企业在数字化转型中充分发挥开源人才的作用。

3.开源人才评价与认证：专栏将探讨开源人才的评价体系设计，包括定性和定量的认证标准。详细研究如何科学公正地进行开源人才评价，并探讨推广开源人才认证的方法，使其成为企业用人和高等教育的重要参考。

4. 开源人才的国际国内形势分析：专栏将关注开源人才在国际和国内的发展状况。分析其面

临的新问题和挑战，以及在全球化合作中所扮演的角色，为读者提供全球开源人才发展的全景图。

5. 开源人才的发展方向和政策建议：专栏将对数字经济的发展趋势进行研究，提出开源人才发展的战略性建议。深入研究政策对开源人才的支持作用，为政府和企业提供合理的政策建议。

6. 开源人才的全球化合作：专栏将聚焦于开源人才在全球范围内的合作机会和挑战。深入研究全球化对开源人才的影响，推动开源社区和企业之间的协作，促进全球数字化共享。

专栏将邀请国内外知名专家学者、企业实践者等，共同探讨开源人才发展的理论和实践问题，为数字经济时代的劳动力和生产力的匹配契合度提供理论的支持。

2）专栏的意义

《开源人才观专栏》的意义主要体现在以下几个方面：

· **理论意义**：专栏将为开源人才发展的理论研究提供新的视角和思路。专栏将从多个维度分析开源人才的定义、特征、价值主张、培养、使用、评价和激励等问题，为开源人才发展的理论研究提供新的素材和见解。

· **实践意义**：专栏将为开源人才的培养、使用和评价提供指导和建议。专栏将分析国内外开源人才发展的典型案例，为企业、个人和政府提供开源人才培养、使用和评价的参考和借鉴。

· **社会意义**：专栏将促进开源人才的发展，推动数字经济的发展。专栏将为开源人才的培养、使用和评价提供支持，为数字经济的发展提供人才支撑。

通过深入了解开源人才观，读者可以获得提升企业竞争力和创新能力的关键策略和方法，同时也可以为个人的职业发展提供指导和启示。

3）专栏的目标

《开源人才观专栏》的目标是专注于开源人才各个方面的研究，提供开源人才发展领域研究的专业指南，推动开源人才观的深入研究和实践应用。具体目标包括：

· **提供实用的指导和建议**：专栏将关注实际问题，提供创新性和实用性的建议，助力教育机构、企业和政府更好地培养和利用开源人才。

· **推动开源人才认知升级**：通过对开源人才观念的传播，促使个人、企业和社会更好地理解和认知开源人才，推动其在数字化时代的重要性。

· **构建开源人才发展体系**：帮助构建完善的开源人才发展体系，推动开源人才观的理念深入

· **为政策提供支持**：提供对开源人才政策的专业研究和建议，为政府和企业在人才培养和应用方面提供有力支持。

· **促进全球化合作**：关注开源人才在全球范围内的发展，推动国际合作，促进全球开源社区和企业之间的交流与协作。

开源人才观专栏将致力于成为开源人才发展的理论研究和实践交流的重要平台。专栏将不断完善内容，邀请更多专家学者和实践者参与，为开源人才的发展做出更大的贡献。

2. 开源能力框架介绍

开源能力框架是一个关于如何理解、培养、评价和激励数字人才的参考框架。它借鉴了开源软件的理念和实践，强调人才的共享、协作、创新和贡献，以及人才的自主、自由、自律和自我提升。

图一：开源能力框架设计

1）开源能力框架的关键要素

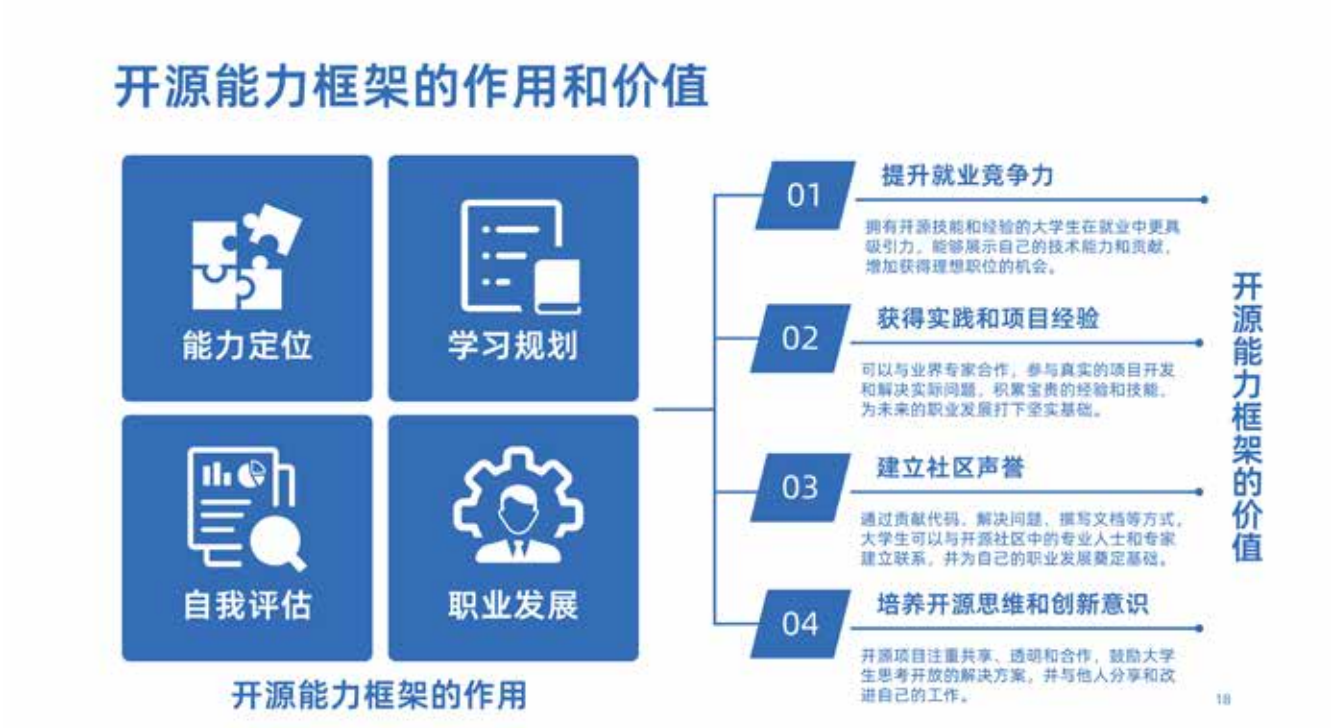
开源能力框架是一个用于描述和评估开源人才的能力的工具，框架的关键要素包括：

	关键要素	要素说明
1	能力领域	开源能力框架将开源参与者所需的能力分为不同的领域。这些领域可能包括技术能力、沟通与协作能力、项目管理能力、开源许可与合规能力等。每个领域代表了参与开源项目所需的特定方面的能力。
2	能力描述	对于每个能力领域，开源能力框架提供详细的能力描述，包括该领域的核心概念、技能要求和能力水平的不同层次，帮助参与者和组织了解每个能力领域的具体要求，并评估其自身在每个领域的能力水平。
3	能力级别	开源能力框架将能力划分为不同级别或层次，反映了从初级到高级的能力进展。每个级别对应着特定的能力水平、技能和知识要求。参与者和组织使用这些级别评估和衡量自己在每个能力领域中的能力水平。
4	能力培训	开源能力框架还提供了相关的能力培训和资源。这些培训和资源可以帮助参与者和组织学习和发展所需的开源能力。培训可以包括技术培训、法律和合规培训、项目管理培训等，以提供全面的能力发展支持。
5	能力评估	开源能力框架提供完整的评估模型，通过能力评估，参与者和组织可以了解自己在每个能力领域中的强项和发展需求。根据评估结果，可以制定相应的发展计划和培训计划，以提高在开源项目中的能力水平。
6	能力认可	开源能力框架提供能力认证和认可机制。这些机制可以通过评估和验证参与者在特定能力领域的能力水平，为他们提供能力认证或获得特定的认可标识。这有助于参与者证明自己在开源领域的能力和信任度。

图一：开源能力框架设计

2）开源能力框架的作用

开源能力框架是指导开源人才培养、使用和评价等工作的基准，可以为开源人才的发展提供方向和指引。



· 对于个人能力提升：帮助个人通过参与和贡献开源项目，提高自己的技术水平和创新能力，同时也增加自己的影响力和收入。

· 对于企业用人、构建核心竞争力和实现数字化转型：帮助企业通过招聘和培养开源人才，提升企业的技术创新和竞争力，同时也促进企业的开源文化和价值观。

· 对于开源社区的贡献增长：帮助开源社区通过吸引和激励开源人才，增加开源项目的数量和质量，同时也提高开源社区的活跃度和声誉。

· 对于开源生态价值创造：帮助开源生态通过整合和协作开源人才，创造更多的开源产品和服务，同时也扩大开源的影响和意义。

· 对于国家数字化战略发展：帮助国家通过培育和支持开源人才，推动国家的数字化转型和创新，同时也提升国家的数字化竞争力和地位。

·对于参与全球化合作：有助于连接和吸引全球开源人才一起协作，促进全球的技术共享和协作，加强我国与其他国家在数字化领域展开深入合作，共同推进科技进步和全球经济可持续发展。

3. 专栏文章预告

《开源人才观专栏》即将推出一系列关于开源人才发展的专题报道，深入剖析数字时代开源人才培养、使用、评价和激励，预告系列包括概览、价值主张、战略管理、能力发展、评价体

1.《开源人才观概述篇》：介绍开源人才观的基本概念，阐述其在数字经济时代的背景和重要性，为后续深入探讨提供基础。开源人才观指的是将人才视为一种可共享的资源，强调人才流动的便利性、多样化和包容性。在这个框架下，人才不再被视为某个特定组织的私有财产，而是可以在不同组织间流通和共享的资源。

2.《开源人才观的价值主张分析》：分析开源人才观在数字经济中的核心价值主张，探讨其对企业和个体的积极影响，为建立开源人才观的合理性提供理论支持。开源人才观打破了人才流动的壁垒，实现了人才的高效配置。通过实现人才资源的共享，可以提高人才的使用效率和效益。

3.《开源人才的战略管理框架》：提出战略性的开源人才管理框架，包括愿景、战略、执行和评估等核心维度，以及它们之间的关系和对齐。企业应该制定并执行开源人才的战略计划，包括招聘、培养、激励和留住开源人才。

4.《开源人才的能力发展模型》：为了实现开源人才的优势互补和协同发展，需要建立相应的能力发展模型，明确开源人才的技能阶段和发展路径，提供有针对性的培训和发展平台，以满足不同类型人才的需求。

5.《开源人才的评价体系设计》：设计全面的开源人才评价体系，包括多维度的评估标准，为人才绩效评估提供科学依据。评价体系的设计应包括构建全面的评价指标和标准、采用多元化的评价方法和手段以及注重评价结果的分析和应用，以不断优化人才资源配置和提高人才管理水平。

6.《开源人才的“第五项修炼”实践》：借鉴彼得·圣吉的“五项修炼”理论，如跨团队协作、开放创新思维等，帮助开源人才更好地适应数字经济时代的复杂环境。通过实践开源文化和价值观，开源人才可以不断提升自身的能力和影响力，成为数字经济时代的领军人才。

欢迎专业人士和研究者投稿，共同探索开源人才观的未来。

4. 专栏编辑寄语

专栏特约研究员：郭皓

开放原子开源基金会资深研究员，开放原子开源教育资源仓Maintainer，开源理论研究者、开源技术和文化布道者。聚焦于开源人才观的核心理念，围绕开源能力的培养、社区参与、技术创新等方面展开深入研究。希望为读者提供全面、深刻、实用的前瞻性的理论探讨和案例分析，助力开发者和组织在数字经济时代更好地适应和成长。

企业开源人才需求
—通过招聘看企业开源策略

微众银行招聘开源社区运营

【岗位职责】1、围绕开源社区运营指标（用户数、贡献者数、影响力等），策划开源社区用户成长体系和影响力塑造方案，实现各层级用户的增长突破，并例行输出周期性运营报告及改进建议；2、负责社区内共建伙伴/潜在共建伙伴的拓展与对接，挖掘产业应用落地合作机会；3、深入整合伙伴资源、挖掘和提炼社区成果，通过官方阵地及媒介渠道，打造社区品牌知名度和影响力；4、密切关注和洞察行业动向，根据市场趋势及时调整运营推广方案，并驱动内部相关团队针对市场变化做出响应。

【任职要求】1、本科及以上学历，有开源社区运营、产品营销、市场策划等相关工作经验优先；2、以用户为中心，具有较强的服务意识和沟通技巧，能有效洞察用户需求，有知名技术社区运营或区块链行业从业经验优先；3、具有较强的文案撰写、整合营销传播能力，熟悉科技产业发展，具备TO B营销经验者优先；4、结果导向、高执行力、沟通能力强，擅长自我驱动，具备强大责任感和团队合作精神。

简要分析

虽然没有看到微众银行的这次招聘的具体项目，但是我们可以从历史信息中得知微众银行已经开源的几个项目，领域涉及Blockchain、隐私计算等，从此次发出的JD来看，其实抛开开源二字，和通常公司招聘的运营也没什么差异，这是常见的一种将开源视为用户社区的策略。

零一万物招聘开源社区运营

【岗位职责】1、负责开源项目社区运营工作执行，包含社区内容策划，活动组织、跟进及落地；关注社群规模、开发者/用户的活跃度和转化。2、完成技术类讲座、内容组织、专题技术节等活动；并针对线上/线下活动的策略探索，不限于直播、Meetup、线下沙龙、分享会。

【任职要求】1、开源社区运营经验优先，类似的科协、校园技术类活动优先；2、对开源、大数据、云计算和AI领域有了解优先；3、计算机相关专业、新闻传播类专业优先；4、对Twitter、Github、Hugging Face相关开源社区大V有资源链接优先。

简要分析

零一万物是创新工场孵化，李开复创始的AI大模型公司，近期要发开源大模型。在“百模大战”的今天，开源作为创业公司的一个生存或拓展市场的策略，可谓是具有非常具有挑战的事情。但是究竟能否利用好开源，还要看整体的策略与决心。

OSPO——数字化政府的新工具

欧洲开放论坛

欧洲开放论坛（OFE）[1]是总部位于布鲁塞尔的非营利性独立智库，它向欧洲各地的政策制定者和共同体组织讲述计算开放性的优点。

OFE最初发起于2002年，旨在促进和扩大企业、消费者和政府对开源软件（OSS）的使用，此后其关注领域不断拓展。OFE目前在布鲁塞尔设有一支政策研发团队（Policy Research and Development team），该团队由我们的支持者联络网和专门的专家顾问提供支持。我们的主要政策主题覆盖：开源、开放标准、数字化政府、公共采购、知识产权、云计算和互联网政策。

OFE还拥有由开放论坛学院研究员（OpenForum Academy Fellows）组成的独立全球联络网，每位研究员都在核心主题上贡献了重要的创新思维领导力，以对影响ICT市场开放性的关键问题提供新的意见和见解。OFE直接或通过其国家伙伴与欧盟委员会、欧洲议会、国家和地方政府密切合作。

The OSPO Alliance
OSPO联盟

OSPO联盟（The OSPO Alliance）由多家欧洲的非营利性组织（OW2、Eclipse基金会、欧洲开放论坛和公共代码基金会）及相关个人在2021年6月发起，旨在丰富管理开源软件的优秀方法。我们一起创建了OSPO.Zone[2]——一个开放的经验共享平台，以促进对于工具和最佳实践的探索，并帮助定义该领域的最新技术。

OSPO联盟旨在为所有愿意就开源软件的使用、贡献和发布进行专业化管理的组织提供可操作的指引和解决方案，不论组织的规模、收入模式，也不论其在公立还是私立领域。特别是，它将帮助这些组织在其信息系统与流程中充分利用开源软件势不可挡的进步性。使用开源软件将促进工具和最佳实践的发现和实现。

通过对开源软件进行专业化管理，OSPO联盟将降低使用开源软件的风险，并提高可预测性。它将降低使用开源的障碍，并促使组织可利用它来增强其数字主权。

INTRO AND CONTEXT
前言及背景

各级政府（地方、市、地区、国家和超国家的）都显现一种明确的趋势，即以战略的视角思考开源，以实现更宏伟的目标。开源在技术领域无处不在，这证明、甚至要求大多数数字使能的公立领域就开源采用更为积极、更为广泛的方法。

由于各级政府机构希望更大程度地吸引公民参与，更有效地利用纳税人的资金，并在本土背景下解决全球挑战，开源软件战略方法的价值更为凸显。公立领域和政府数十年来持续采购、使用和贡献开源，政府中开源项目办公室（Open Source Program Office）的兴起，更有望支持公立领域以最佳方式利用其与开放共同体在软件、标准、数据、文化、研究等方面的合作。

精通开源的政府首席信息官（CIO）和IT部门不断意识到，当他们提高其参与、贡献项目与开源共同体的能力时，其可以通过开源而实现的价值就会急剧增加。因此，越来越多的政府CIO选择开源项目办公室（Open Source Program Office）并将其作为提升其组织来满足新旧诉求的能力的工具。

开源项目办公室（OSPO）是一个支持和促进消费、创建和应用开源软件的机构性组织构架。OSPO是一个机构的重心以及开源能力中心，其从战略上实现该机构与开源相关的政策目标。

本文探讨了将OSPO引入公立领域的早期尝试。本文将讨论开源在政府战略背景下的发展，参与开源共同体的价值，以及OSPO在提供专业知识和联系方面对于彰显全球化协作及共同创造的价值的潜在作用。本文认为OSPO是一个多面工具，其用于解决不同公立领域的高管在不同角色中所面临的挑战，并满足这些高管使用开源软件（OSS）的诉求。因此，本文主题是公立领域的组织化能力建设。

下述案例研究是基于对公立领域OSPO领导者的采访，并调研他们为什么以及如何建立OSPO。这些案例研究概述了不同OSPO的责任及活动，并探讨了OSPO实现一系列政策目标的潜力。

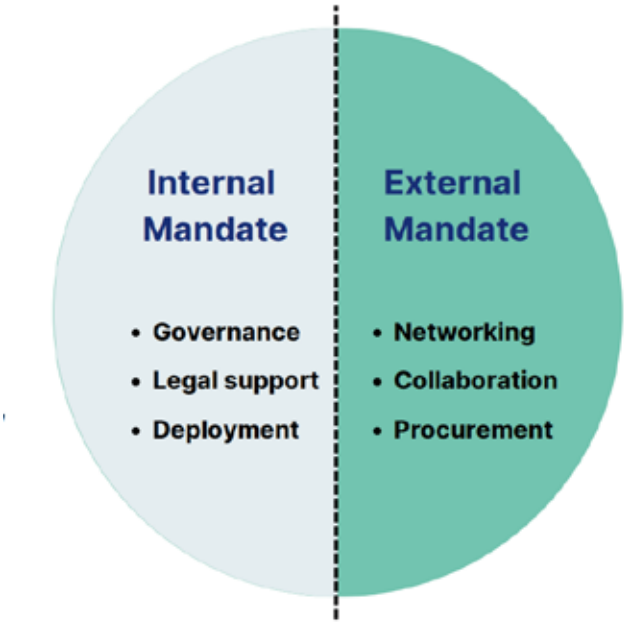
建立OSPO的趋势是对数字化政府所面临的更广泛趋势的回应。公民和政客要求提供更开放、更负责任和更容易获得的高质量服务。他们要求在严格的预算限制下实现这一目标，同时保持数字主权、系统韧性及网络安全。开源在这个不断变化的环境中扮演着重要的角色，且OSPO是政府CIO利用开源软件满足诉求的工具。对于这些复杂挑战，OSPO是数字化政府应对这些复杂问题的新工具。

在私立领域建立OSPO对于大规模创新和共同创造必不可少。建立OSPO后，企业已经找到了如何通过开源释放大量价值从而让全球股东受益的方法。本文发现，公立领域的价值立场与之密切相关，但又本质上不同。

本文还探讨了现代OSPO的职权。它需要在开源软件的合规性、安全性和治理方面上提供内部价值。

至关重要的是，应为OSPO创建具有与外部开源生态系统进行交流及合作的职权。它需要成为一个接口，支持和管理整个组织与外部利益相关者之间在信息、思想、软件贡献、关系及采购活动上的交流。

本文的目的不是概述各级政府CIO所面临的各种挑战和障碍的解决方案。相反，本文的主要结论是，OSPO的建立是为了给政府CIO在软件产品和服务方面提供务实的选择、灵活性和控制权，反过来又使他们能够更好、更有效地满足对其提出的各种复杂诉求。



Paper Structure and Definitions
报告结构和定义

这篇报告可以看作是欧盟委员会发布的开源对欧盟经济的影响报告——“开源软件和硬件对欧盟经济的技术独立性、竞争力和创新的影响”的后续，其中包括支持在欧盟公立领域和学术界中建立20个OSPO的政策建议。

在公立领域建立OSPO是一项飞速政策创新。为了介绍这一领域的情况，本文自由穿梭于当下的实践和理论之间；OSPO是什么以及它能成为什么。本文并未呈现组织化的模式、标准方法或“最低可行的OSPO”，而这将是后续报告的主题。

开源产品和服务的采购也并非本文重点。OSPO将在有效的开源采购中扮演重要（甚至是关键的）角色，但是对于那些仍在争论是否要采购开源的组织来说，建立OSPO就不那么重要了。正在建立OSPO的组织往往已经超越了仅将开源用于节省成本的旧模式，而是着眼于他们的战略方法，以实现价值、创新和灵活性的最大化。

我们所说的“开源软件”，是指在开放源代码促进会（Open Source Initiative）批准的许可证

符合开源定义的软件；简单来说，用户可以访问、修改并改进源代码。

本文多处提到“共享与复用”。对此，我们指的是任何人都可以访问源代码，根据需要进行修改，并通过重新发布这些改进以供人们使用。

本文交替使用“公立领域”、“政府组织”、“公共实体”和“公共机构”，这样做是为了强调OSPO概念与全部或部分由国家控制的所有经济部门广泛相关。

同样，本文所说的“政府CIO”指的是公立领域的组织中为支持组织和政治目标而负责信息技术和计算机系统的职位。这包括首席数字信息官（CDIO）或IT部长等角色。他们将是负责建立OSPO的最高级的管理人员。

最后但同样重要的是，作者要感谢支持本文撰写的专家组:

Bastien Guerry, Government of France

Clare Dillon, InnerSource Commons Foundation & OSPO++

Danese Cooper, InnerSource Commons Foundation & OSPO++

Deborah Bryant, Independent Advisor & Open Source Initiative Board Emeritus

Frederik Blachetta, Dataport

Gal Blondelle, Eclipse Foundation

Gijs Hillenius, European CommissionJacob Green, Mosslabs.io, OSPO++

Jacob Green，Mosslabs.io，OSPO++

James Vasile, Open Tech Strategies

Johan Linker, RISE Research Institutes of Sweden

Leslie Hawthorn, Red Hat & Open Source Initiative Board Emeritus

Mala Kumar, GitHub

Michael Plagge, Eclipse Foundation

Miguel Diez-Blanco, European Commission

Philippe Bareille, City of Paris

Richard Littauer, Open Source Collective and Sustain

Sayeed Choudhury, Johns Hopkins University & OSPO++

公立领域与开源

城市与国家政府的诉求往往有所不同。税务机关与超国家组织（例如欧盟）也有着不同的授权。公立领域采购、使用和部署开源解决方案的原因是多方面的，很难像公立领域这种宽泛的领域一概而论。但是，无论是有意还是无意，所有公立领域的组织都在使用开源软件。公立领域早期使用开源的应用程序和工具通常是为了完成没有资金支持的政策职权（即，需要完成一个新项目或达成新能力，但没有相关预算）以及减少采购摩擦而做出的一种机敏的反应。

出于战略目的使用开源的原因在于，在开源软件许可证下的软件易于检查、互操作、共同创造，具有扩展性、可持续性和可定制化，而专有的解决方案无法提供这些优势。例如，如果你有6万所学校需要软件解决方案，那么为开发与支持软件而提供资金比为每所学校支付许可费要更佳。公立领域使用开源的原因有（但不限于）：

· 透明度与信任
· 节约成本
· 避免软件供应商锁定
· 增加采购过程中的中小企业
· 互操作性
· 公民参与
· 减少政府内部和政府之间的合作摩擦
· 利用最先进的技术
· 提高政府组织的能力和技能
· 吸引并留住人才
· 行业和政府组织合作的新兴方式

在“开源”这个词被创造出来之前，公立领域就已经使用开源了。以本文提到的组织为例，在2000年12月，欧盟委员会就制定了一项关于内部使用开源软件的战略。巴黎市参与开源也已超过

增加公立领域对开源的使用

组织诉求

· 系统的功能

· 开发和保留技能

· 需要分担开发、创建、 维护、发展、问题响应、安全和开发技能的成本

政治诉求

· 网络安全/弹性

· 数字主权

· 经济发展

· 共享/复用

· 预算约束

公民诉求

· 开放/透明的信任

· 有效利用资金

· 政府服务的质量

· 公民参与

可以说，由于上面列出的诉求，公立领域使用开源的趋势有所增加。值得注意的是，每个诉求的重要性（这个列表远没有详尽列举）将因国家、政府组织形式和参与开源的历史而异。在对CIO提出的诉求中，存在5个突出的战略要素。

数字主权

数字主权的概念是多个司法管辖区关于数字政策辩论中的关键议题之一，原因在于政府已经意识到对某些软件解决方案的过度依赖及有限数量的供应商的能力。开源，特别是当它与基于开放标准的采购流程结合时，它为公立领域的采购机构提供了真正的选择，并避免了供应商锁定[4]。这并非一个新认知，但从战略角度来看，整个社会的高度锁定破坏了数字主权。该诉求由政治层面推动。

经济增长

公立领域不能有效使用开源软件所付出的代价，不仅造成更高的货币成本、更低的竞争、不灵活的系统和锁定，还有存在于经济增长中巨大的机会成本。欧盟委员会关于开源对欧洲经济的影响研究概述了政府发布、使用和贡献开源软件带来了经济增长、就业和初创企业等方面巨大的（大部分并未实现的）积极经济外部效应。Frank Nagle关于法国政府决定发布更多代码所做的研究结果[5]也印证了这点，他发现，“这项规定导致使用开源软件的企业每年增加0.6%-5.4%，与IT相关的初创企业数量每年增加9%-18%，从事IT相关工作的人数每年增加6.6%-14%。”该诉求也日益由政治层面推动。

跨境中的互操作性与跨部门公共服务

公立领域不能有效使用开源软件所付出的代价，不仅造成更高的货币成本、更低的竞争、不灵活的系统和锁定，还有存在于经济增长中巨大的机会成本。欧盟委员会关于开源对欧洲经济的影响研究概述了政府发布、使用和贡献开源软件带来了经济增长、就业和初创企业等方面巨大的（大部分并未实现的）积极经济外部效应。Frank Nagle关于法国政府决定发布更多代码所做的研究结果也印证了这点，他发现，“这项规定导致使用开源软件的企业每年增加0.6%-5.4%，与IT相关的初创企业数量每年增加9%-18%，从事IT相关工作的人数每年增加6.6%-14%。”该诉求也日益由政治层面推动。

政府数字服务的透明度和负责度

开源并不是信任和透明度的灵丹妙药，但它增加了公民检查、交互组成数字服务的代码的能力。该诉求由公民自身和政客推动。为了实现数字化政府的承诺，公民必须信任被提供的服务。总体而言，社会趋势正在使得对于公民参与度、中小企业参与度以及提高政府运作透明度和负责度的诉求增加[6]，数字服务也是如此。

技能和人才招募

所有组织（无论是在私立领域还是公立领域）都在努力寻找技术人才。在私立领域，开源已经陡然发展，因其允许开发团队（并通过扩展到企业）分担开发、创建、维护、发展、问题响应、安全和开发技能的成本。此外，开源是开发者的首选，因为在他们交付高质量代码的同时，开源提高了他们更快速地迭代解决方案从而解决技术难题的能力。

OSPO的深入解析

随着人们对开源软件和当今的CIO的诉求越来越大，OSPO迎来了发展机遇。对开源软件的诉求已远远超出了开放代码的范围，该诉求延伸到组织文化、对开放性和透明度的承诺，以及最重要的合作方面。当我们谈及数字政策与软件，我们谈论的是开源。它是数字世界的基础创新层。对于CIO来说，OSPO是他们的组织与该层之间的接口。

OSPO是私立领域的既定概念。当前，越来越多的学术和政府部门也在设立OSPO。OSPO是一种制度性组织结构，它支持并促进消费、创建与应用开源软件。它是机构中的中心办公室，致力于实现该机构与开源相关的政策目标。

根据其部门、规模和类型的不同，组织的开源目标也会有所不同。各组织建立OSPO是为了实现这些目标，因此所有的OSPO各不相同。

在私立领域建立OSPO，对于找出如何通过开源释放大量价值并刺激创新从而使全球股东受益的方法来说至关重要。OSPO的兴起是今天开源无处不在的直接结果。事实上，92%的应用程序都使用了开源组件[7]。

企业建立OSPO是为了提供必要的能力、技能及共同体参与，以便其以有意义的方式成为开源生态系统的组成部分。OSPO回应了如下认知：使用开源不再是一项选择，而是必需。

大型企业已经在学习并采用开源开发所特有的流程及方法上投入了精力与资源。

私立领域OSPO的大多部门都能适用于政府，而政府OSPO可以（也应该）开展更宽泛的工作。因为公立领域对公民的责任比企业对股东的责任更大。从这个角度看，OSPO一方面可以推动开源目标的实现，另一方面也可以满足需要开源的更宽泛的政策目标。

换句话说，OSPO的职权应该包括软件开发和维护的日常事务，但它可以（或也应该）支持

实现全面的政策目标，如隐私、安全、认证、多样性、公民参与及技术获取。

以前的OSPO是专注于内部的，现代OSPO则有明确的内部和外部职权。下文的概念图基于OSPO++联络网的工作模型，显示了OSPO是组织与其他同行OSPO及开源生态系统中（及之外）的其他人的协作接口。

内部职权

OSPO对组织有一个横向的展望，使其可以有效地利用现有资源。下文列举了在OSPO内部职权范围内的活动实例，包括实现开源软件开发的最佳实践和网络安全所需的适当工具、平台和实践。此外，OSPO的内部职权支持了组织内部开放文化的发展，这超越了软件和数字基础设施建设的层面。它是作为文化变革的工具而建立的。欧盟委员会的OSPO明确发挥了这一作用，微软的OSPO可以被视为“OSPO文化变革”的私立领域例子[8]。

在OSPO内部职权内的活动实例包括：

- 确保合法合规
- 制定和实施开源软件战略
- 帮助启动新软件项目的团队更好地使用开源
- 数字化合作战略
- 衡量组织对开源软件的使用和进展（指标和统计数据）
- 为开源软件制定募资方案
- 为员工提供培训和指导，让他们了解如何参与开源软件活动
- 在内部宣传和交流有关开源的倡议，以及组织参与开源的任何其他活动。

外部职权

OSPO需要在内部职权下为其服务的组织提供直接价值。然而，由于开源的本质，启用OSPO的组织意味着成为共同创造价值的共同体的一部分。因此，现代OSPO有一个重要的外部职权，即确定新的项目、工具、行动者和实践，从而改善OSPO和整个组织的工作、效率和未来战略。正如案例研究所示，政府官员和OSPO参与者经常认为这一外部职权是OSPO在支持组织方面的最关键特征之一。

另一方面，当外部开源开发者和项目想与公立领域的组织进行开源合作时，往往会面临一个挑战：如果他们想讨论一个潜在的解决方案，或者不确定与政府管理的数字解决方案有关的许可问题，那么他们该与谁联系？这可能而且应该超越了代码层次。OSPO便可以提供这样一个接口：为其他政府官员、开发者和开源项目，以及为国内和全球的其他OSPO提供一个入口。

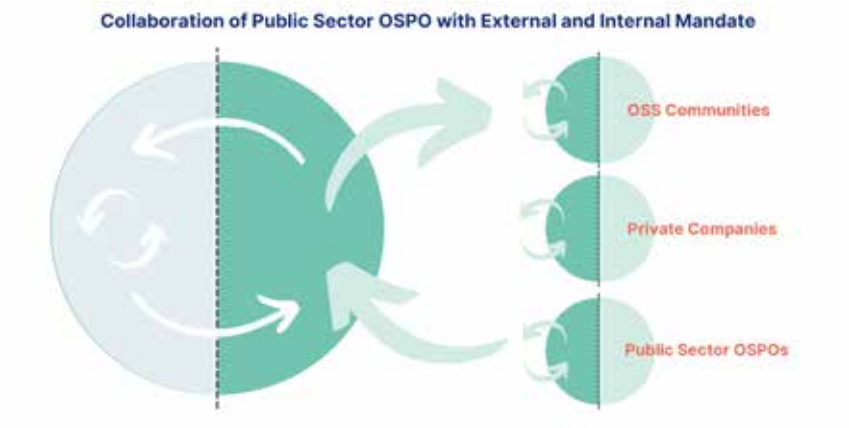
当涉及到组织的日常活动时，政府OSPO的外部职权可以协助组织在政策、采购、IT和供应商以及在采购过程中合作的其他公共组织之间进行沟通与翻译。这在市政一级尤为重要和明显。

采购将激活内部和外部职权。可以说，这将是OSPO能为公立领域的组织带来的最大货币价值。OSPO的建立增加了支持有效采购开源软件产品和服务的能力与资源。OSPO可以帮助确定开源替代方案，根据诉求和规范评估产品和服务，评估开源软件项目的健康和安全，计算所有权的总成本，并确定定制化与集成的需求。

在OSPO外部职权内的活动实例包括：

- 安全、可持续地接受和提供外部代码贡献
- 对外宣传及交流有关开源的倡议，以及组织参与开源的任何其他活动
- 与基金会/组织和开源共同体开展合作
- 提供对开源领域已开发的替代方案的认识及认知，以避免不必要的重复
- 管理生态系统中开源利益相关者的多样性
- 支持开源软件产品和服务的采购
- 实现软件的共享和复用

一个重要的改进点是：作为接口的OSPO不应该创建额外的官僚阶级，它应该是一个推动者。换句话说，不是所有事情都需要通过OSPO。



政府OSPO支持组织内部以及整个组织与外部利益相关者之间的代码、思想、采购活动、信息和知识的交流，它是一切“开放”的通用接口。私立领域花了几十年的时间来构建OSPO的内部和外部职权，对政府来说，其任务更明确，即是合作而非竞争，这应该是理所当然的事情。

公立领域OSPO的案例研究
欧盟委员会OSPO

欧盟委员会宣布将于2020年10月建立一个OSPO（EC OSPO[9]）。这是其2020-2023年开源战略介绍的一部分。欧盟委员会将开源战略的这一迭代公布为“委员会通讯文件”，使其成为整个欧盟委员会的战略，而不仅仅是IT总署的战略。这也使OSPO获得了更强的政治任务。

EC OSPO致力于实现开源战略中概述的愿景及目标：“欧盟委员会利用开源的变革、创新和协作能力，鼓励软件解决方案、相关知识和专业知识的共享和复用，从而提供更好的欧盟服务，丰富社会并注重降低社会成本。”

EC OSPO是欧盟委员会内部文化变革的一个工具。它的作用是“加强和扩大开源文化[10]”。它隶属于“信息总署”，但旨在支持所有的总署，并在政治和组织上得到支持来这样做。这是因为软

件的开发、使用和普及涉及整个机构。OSPO应该在这些团队和项目之间开展工作，使欧盟委员会所开发的源代码可供所有的开发团队使用。这项工作首先在欧盟委员会内部进行。目前，OSPO正在努力消除已识别的法律和技术障碍，以便欧盟委员会在OSPO的支持下公开提供更多的解决方案。

欧盟委员会希望利用OSPO为自己做好准备，逐渐接受来自组织外的开源贡献，并开放面向更广泛的合作。以上贡献与合作都可以超越代码层面。OSPO和该战略还承诺积极支持欧盟委员会之外的开源开发者共同体。实际上，OSPO的目标是连接和参与开源共同体和项目，特别是那些为欧盟委员会所依赖的工具做出贡献的共同体及项目，例如Drupal[11]。

> **译者注：Drupal是开源软件，目前由超过63万使用者和开发者共同维护和持续开发。Drupal遵循GNU通用公共许可协议，每个人都可以免费下载、分享使用。在这种开放的开发模式下，开发者可以持续引进网络发展中的最新技术，使Drupal成为技术领先的平台。Drupal的原则是鼓励模块化、标准化、合作、易用性等。Drupal共同体提供支持的方式多种多样——聊天工具、论坛、在Drupal大事件期间面对面交流。共同体还为Drupal创建了文档，涉及到使用Drupal的主要话题。Drupal全球共同体引领着各项创新，使Drupal越来越被网络开发者和站长们偏爱。每个人都可以参与到Drupal共同体中来，并作出贡献。**

EC OSPO表明，一个政府的OSPO不必规模庞大或成本高昂，也能产生影响。欧盟委员会约有32000名员工，OSPO最初的团队只有两个人。随后，欧盟委员会加强了OSPO，新聘人员带来了更多机构管理的知识和能力，其主要职责是在组织方面发展EC OSPO。

在欧盟委员会20年来不断加大开源方面的工作下，EC OSPO顺理成章的成为下一阶段的工作。尽管如此，该战略的制定者对在欧盟委员会内设立OSPO仍有大量考虑，这个想法已经在该机构与开源关系最密切的官员中流传了数年之久。成立前的一个关键过程是由外部咨询企业对欧盟委员会的开源治理和采用情况进行调查[12]。在这项调查中，OSPO的成立建议是通过与私企、政府和民间社会组织的对话中达成的。更具体地说，它建议成立一个作为“企业管理的最先进结构”的EC OSPO。这是基于法国国家层面的政府和谷歌的开源项目办公室所采取的举措。

法国政府OSPO

和欧盟委员会一样，法国政府长期支持推广和使用开源。多年来，它在公立领域实施了若干支持开源软件的政策，例如，5608号通函（Circulaire 5608）[13]要求所有公立领域在采购时首先考虑开源。法国政府OSPO成立的契机是2020年Bothorel报告[14]的发布。这份文件是法国议会的成果，它建议设立一个国家级OSPO。2021年，公共转型与民事服务部部长宣布成立OSPO，并宣布一系列在公共行政部门内推广、采用和改进开源软件的行动。

新OSPO（Pole d 'expertise logiciels libres[15]自由软件专家中心）是首个为国家政府设立的此类机构之一。它隶属于跨部委的数字总署（DINUM[16]），因而支持法国政府的所有部门。与EC OSPO类似，法国政府OSPO从一份开源战略文件“Pland' action logiciels libres et communs numériques[17]自由软件与数字共同体的行动计划”中获得授权。简而言之，法国OSPO致力于提高公立领域对开源软件的认知、使用及发展。

法国政府OSPO的一个重要既定目标是增强作为雇主的公立领域对具有数字技能的青年人才的吸引力[18]。它通过与法国政府的开源开发者共同体“BlueHats”合作，组织年度“自由与开源冲刺”活动，同时也通过使用开源本身来实现这一目标。因为开发人员和软件工程师不太可能选择让其使用和贡献开源能力受限的工作。

OSPO将参与几项宏伟的计划。例如，政府投入3000万欧元资助地方政府的开源解决方案。在开发方面，它将与法国网络账号联通平台France Connect合作公布平台的源代码。此外，它将运行开发code.gov.fr网站（也有英文版本）。它还推出了“BlueHats代码学期（BlueHats Semester of Code）”项目，软件工程专业的学生将贡献开源软件6个月。

建立联络网对国家OSPO具有特别重要的意义。法国OSPO团队表示，他们不能忽视在城市、市政机关、大学和其他组织所做的工作。这些经验带来了一个重要的观点：OSPO的参与确保了资源的有效配置、创新及改善。因此，有必要在中央OSPO和不同的机构/组织之间建立强大的协作和联络网机制。

OSPO团队表示，发掘共享和复用开源解决方案的潜力是关键的开源挑战。他们非常需要了解所有可用的开源资源，以便政府的其他部门可以使用它们，并避免重复。该需求也延伸到了城市、乡镇和直辖市，且在软件产品方面往往也有类似的需求。此外，还需要帮助机构开发和维护这些解决方案，以寻找新用户。他们的目标是提供一套现成的解决方案，可供不同的公立领域的用户和组织轻松下载和安装。

然而，OSPO面临的最大挑战与一般的政府CIO面临的类似：满足不同的诉求和需求。OSPO要满足许多公立领域的诉求与需求，包括各部委、部门、实施部门和地方公立领域机构。换句话说，OSPO既有支持政府参与开源的内部职权，也有与城市、市政当局、大学和其他实体合作的外部职权。

巴黎市OSPO

巴黎市OSPO于2021年11月宣布成立，其最重要的目标是成为公共行政部门、共同体用户和其他项目、倡议之间的接口。在建立巴黎OSPO的过程中，一个突出特色是它是一个自下而上的项目。它由市政厅的一群热心人士推动。巴黎市OSPO发展历程中的一个契机发生在2002年，当时市议会投票赞成开放Lutece平台[19]。巴黎市在过去的20年里提出的大部分开源倡议，以及现在建立OSPO的想法，都源自于这个项目。

与欧盟委员会一样，巴黎市政府在OSPO成立之前就与其他机构进行了多次交流。例如，在宣布成立之前，巴黎市政厅的团队就参与了OSPO倡议中的OSPO++[20]和OSPO联盟[21]。这反过来又使得与其他OSPO建立联系的文化从一开始就融入了巴黎市OSPO的思维方式和工作方法中。

巴黎市要求其OSPO提升参与开源共同体的能力。这样做的目的一方面，是为了加强围绕Lutece的共同体，另一方面，这也是向其他OSPO、开源共同体和他们自己的行政部门传达巴黎市对开源事业的认真度和专业度。

虽然关注外部共同体和联络网很重要，但巴黎市OSPO强调，它首先致力于加强自身能力。

他们希望将其内部的开源流程正规化，例如许可证合规性审计，并且他们必须为城市的信息技术管理增加价值。他们表示，对于OSPO为之工作的现代公立领域CIO来说，开源已经是日常事务的一部分，但城市需要更多的组织结构来最大限度地利用开源。OSPO的内部职权是制定合规性、技术能力和经验方面的政策，以便组织能够逐渐充分参与到开源生态系统中。为了使这内部职权可付诸行动，巴黎市OSPO正在采用定制版的国际开源共同体OW2的善治（Good Governance）倡议指引。OW2善治倡议旨在通过实施组织范围内的政策，增加对如何使用和贡献开源的认知和专业知识，它为在组织内实现开源项目办公室提供了蓝图。

巴黎市建立OSPO以增加其数字主权和技术自主权。巴黎OSPO团队表示，理论上，通过外包供应商和授权软件来建设城市的数字基础设施成本更低，也更容易。但这意味着失去了对数字资产的控制，而且政府参与技术的能力会逐渐下降，是过度依赖和技术封锁的根源。避免这种情况的发生是政客、高级公务员和公民对数字主权的政治诉求，这也是设立OSPO的一个重要驱动力。

展望未来几年，巴黎OSPO团队看到了创建城市OSPO网络的巨大潜力。城市是数字化政府服务的主要提供者，而且往往会通过与国家政府不同、更直接的方式提供服务。但是要实现巴黎市制定的开源目标，现有的大部分国家层面的倡议都不能完全满足他们的需求。城市应开展具体的合作，重点是经验分享、共同测试想法、程序，也许最重要的是软件本身。

然而，对于公立领域来说，开源不仅仅是代码和信息技术管理。虽然OSPO是一个实用的概念，有助于实现开源参与，但巴黎OSPO团队认为它是数字公地（digital commons）和公共产品这一更大理念的一部分。共享软件很容易，但复用却很难。城市OSPO的目的是为了避免不必要的重复。因此，应该建立一个城市间OSPO联络网，以降低共享和复用数字化政府解决方案的交易成本。巴黎市为此采取了实施OSPO++合作模式的方法，是对于网络化OSPO的最大承诺。

OSPO网络实现软件共享和复用

从案例研究中可以明显看出，OSPO对公立领域的价值主张与对私立领域的价值主张密切相关，但又存在根本的不同。

私立领域的OSPO花费了十多年的时间，超越了法律和支持部门，发展成为支持企业间交流合作的代理组织。如今，我们在OSPO联盟和TODO小组[22]等机构都可以看到企业OSPO的联络网。

建立OSPO的公立领域的组织从一开始就计划从外部来使能它们。一方面，这是因为，与私立领域相比，公立领域的内部资源相对有限。然而，另一方面，由于公立领域有某些特定的项目需求，合作对他们来说应该更理所当然。像消防、警察和图书馆这样的公立领域就是典型的例子，除此之外也可能包括一般的数字服务。

值得注意的是，有无数合作网络旨在促进各级公立领域的组织在速度和规模方面的合作。然而，从开源或更普遍意义上的数字化政府的角度来看，合作的潜力并没有得到充分挖掘。对开源合作来说相当独特的一个有趣的使能因素是，它为合作提供了另一种法律依据。公立领域的组织之间正式合作的合同和谅解备忘录（MoUs）是极具官僚主义的，谈判起来也很繁琐。但在世界各地，维护数字基础设施的开源项目已经建立在一个成熟的法律框架上——开源许可证——这个法律框架提供了可信服务。

对于公立领域的开源合作来说，这不仅仅涉及到一个被广泛接受的规范，它更多触及的是潜力，但也有一些合作的例子，它在没有合同或谅解备忘录的情况下就发生了。例如，对巴黎市的Lutece平台的一些贡献是通过Baltimore的约翰霍普金斯大学OSPO提供的，这是美国的第一个大学OSPO。Lutece现在被Baltimore的圣弗朗西斯邻里中心使用[23]。巴黎OSPO和约翰霍普金斯OSPO的团队将此描述为通过非正式渠道进行的合作，但依靠的是所使用的可信的开源许可证。这是OSPO合作的一个实实在在的例子，在没有合同或谅解备忘录的官僚主义的情况下，实现了实际的共享和复用。

这一点很重要，因为在过去的几十年里，数字化政府的软件产品共享和复用的承诺可以说并未得到实现。欧盟委员会OSPO的代表给出的解释是：“共享很容易，复用很难。”此外，欧盟委员会的“IT解决方案的共享和复用框架[24]”，欧洲互操作性框架[25]的不同迭代，以及无数的国家努力，已经建立了提高软件“可复用性”的方法和程序。这无疑增加了复用的可能性，但在公立领域的背景下，OSPO可以被视为实现复用的推动者。复用受到了组织、法律、技术和交流障碍的阻碍：具有外部授权的公立领域OSPO针对所有这四个方面。此外，由于与适当的内部合规结构相匹配，OSPO降低了开源合作的交易成本，同时保持技术自主、风险缓解和稳定性。

观察与总结

希望政府CIO能从本文中得到与他们所代表的组织相关的结论。然而，从案例研究的普遍角度来看，存在一些关于公立领域的开源和OSPO的明显观察结果与大多数政府CIO相关。

开源观察结果

· 开源软件无处不在，且公立领域依赖它

· 公立领域需要评估其开源的使用、合规性、安全性和关键的依赖关系。这可以通过形势研究、矩阵和统计来完成

· 公立领域的组织之间的软件共享和复用前景广阔，但它在很大程度上仍未实现

· 提高公立领域的开源能力和实力有助于实现政治目标，如经济增长、数字主权和网络安全

· 开源节约成本，采购法律和结构也很重要，但要实现全部价值，一个组织需要投资能力和改变工作文化

· 开源对吸引和留住技术人才很重要

OSPO观察结果

· OSPO是且应该是各不相同的，这取决于组织与其目标

· 公立领域与私立领域OSPO的价值主张是不同的

· OSPO是实现开源目标和需要开源的政策目标的工具

· OSPO带来了能力和文化变革

· 目前具有丰富开源软件经验的组织正在建立OSPO

· OSPO需要一个支持组织内部开源进程的职权，但为了使OSPO从开源中实现价值，它需要一个进行外部合作的授权

· 一个OSPO的优良将取决于它所支持的战略

· 在建立OSPO时，要通过现有的OSPO联络网从先前经验中学习，不要重复造轮子

结论

对于设立在政府的OSPO来说，要做出确定的结论还为时尚早。这就是说，一般的情况下，OSPO的建立是为了向政府CIO提供真正的选择。

考虑到从案例研究中所观察到的情况，并站在政府CIO角度的理论考虑，已建成或正在规划的OSPO是就政治目标和公民诉求方面向CIO所提复杂需求的回应。

OSPO是对当今数字现实的回应，在这个现实中，开源无处不在且不可避免。也许更重要的是，它们的建立也是对战略目标的回应，在这种情况下，则需要有目的地使用开源。战略性地使用开源可以提升一个组织、地区或国家的数字主权，并提升该地区在创业、就业和GDP方面的经济增长。对于数字服务本身来说，开源是实现更好的互操作性和质量的工具，而同时它也有助于提高其透明度和负责度。

OSPO是一种制度性的组织结构，它支持并加速在组织内消费、创建和应用开源软件。在一个组织中做好这一点，对于政府的CIO来说，也有助于吸引和留住技术人才。

节省IT成本是在公立领域使用开源的主要原因之一，无论是所有权的购置成本还是总成本。这是一直存在的事实。然而，在各级政府（地方、市政、区域、国家和超国家）建立OSPO的趋势是当今政府CIO从战略上考虑开源的结果，旨在实现更宏伟的目标。

OSPO给政府CIO提供了更多的务实选择。当涉及到他们的日常工作和长期战略目标时，他们给组织的行政人员提供了更多的选择权、灵活度和控制权。这反过来又使他们有能力更好、更有效地满足对他们提出的各种复杂诉求。

更多资源

OSPO联盟

OSPO联盟旨在为所有愿意对开源软件的使用、贡献和发布进行专业化管理的组织提供可操作的指导和解决方案，无论其规模大小、收入模式、以及是公立领域还是私立领域。通过对开源软件的专业化管理，OSPO联盟将使参与开源软件的风险变得更小且更可预测。它将降低使用开源软件的障碍，并使各组织能够利用它来加强其数字主权。

OSPO联盟已经建立并主持了OSPO.Zone——一个开放的经验分享平台，以促进工具和最佳实践的探索，并帮助定义该领域的技术状态。

OSPO++

OSPO++是一个由大学、政府和民间机构的OSPO组成的联络网和合作共同体。它提供资源来帮助创建OSPO，积极讨论如何最好地管理和发展开源项目，以及如何建立持久的可持续的共同体。

TODO小组

TODO是一个从业者的开放共同体，这些从业者旨在创造和分享知识，在实践、工具和以其他方式进行合作，从而成功有效地运行OSPO或类似的开源促进计划。

TODO小组由其1600多名共同体参与者组成，并受到其70多名普通会员支持。

参考链接：

[1]https://openforumeurope.org

[2]https://ospo-alliance.org

[3]https://lutece.paris.fr/lutece/

[4]https://openforumeurope.org/publications/open-strategic-autonomy/

[5]https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3355486

[6]https://www.sciencedirect.com/science/article/abs/pii/S0740624X17300175

[7]https://blog.tidelift.com/open-source-is-everywhere-survey-results-part-1

[8]https://www.youtube.com/watch?v=WDjh_nbAAeg

[9]https://joinup.ec.europa.eu/collection/ec-ospo

[10]https://commission.europa.eu/select-language?destination=/node/9

[11]https://www.drupal.org/european-commission

[12]https://joinup.ec.europa.eu/sites/default/files/custom-page/attachment/2020-05/D10.2_Public%20version%20of%20the%20final%20report%20FINAL.pdf

[13]https://www.legifrance.gouv.fr/circulaire/id/35837

[14]https://www.economie.gouv.fr/files/files/directions_services/cge/Botherel-mission.pdf

[15]https://www.etalab.gouv.fr/accompagnement-logiciels-libres/

[16]https://www.numerique.gouv.fr/dinum/

[17]https://www.numerique.gouv.fr/publications/plan-action-logiciels-libres-communs-numeriques/

[18]https://www.numerique.gouv.fr/publications/plan-action-logiciels-libres-communs-numeriques/

[19]https://lutece.paris.fr/lutece/

[20]https://ospoplusplus.com

[21]https://ospo-alliance.org

[22]https://todogroup.org

[23]https://lutece.paris.fr/lutece/blog/new-contributors-from-the-johns-hopkins-university.html

[24]https://joinup.ec.europa.eu/sites/default/files/custom-page/attachment/2017-10/sharing_and_reuse_of_it_solutions_framework_final.pdf

[25]https://joinup.ec.europa.eu/sites/default/files/custom-page/attachment/2017-10/sharing_and_reuse_of_it_solutions_framework_final.pdf

[23]https://lutece.paris.fr/lutece/blog/new-contributors-from-the-johns-hopkins-university.html

[24]https://joinup.ec.europa.eu/sites/default/files/cus-

tom-page/attachment/2017-10/sharing_and_reuse_of_it_solutions_framework_final.pdf

[25]https://joinup.ec.europa.eu/sites/default/files/cus-

tom-page/attachment/2017-10/sharing_and_reuse_of_it_solutions_framework_final.pdf

Authors/作者：OpenForum Europe & OSPO Alliance for OSPO.Zone

June, 2022 / 2022年6月

译者/Translators：

赵海玲Hailing ZHAO，开放原子开源基金会行业研究员

审校/Reviewers：

李建盛Jiansheng LI 开放原子开源基金会资深顾问

金思含Sihan JIN 开放原子开源基金会助理开源项目运营官

郭雪雯Vanessa GUO 开放原子开源基金会法律顾问

项目介绍：“源译识”翻译项目是由开放原子开源基金会发起的开源公益翻译项目，旨在通过共译凝聚对开源的共识。目前本项目主要涉及开源许可证翻译、开源案例翻译、开源书籍翻译及开源报告翻译等。详情请见：https://atomgit.com/OpenAtomFoundation/translation .

为什么Debian是现在这样?

Debian是一个庞大且复杂的操作系统，也是极具量级的开源项目，距今已有三十年的历史。对于多数人而言，它的某些方面是有些奇怪的。这些特性的形成大多都有充分的缘由，但是想要挖掘出这背后的缘由并不容易。本文试图回答这些问题，并不详细探讨项目的发展历史。

Debian的目标

Debian的目标是成为一个高质量、安全的通用操作系统，仅由自由和开源软件组成，可运行在世界上大多数正在使用的计算机上。

“通用性”意味着Debian应该适用于大多数人的大多数用途，当然，总会出现不适用的情况，但这是一个值得追求的目标。其他的一些发行版专注于特定目的：桌面应用、服务器、游戏娱乐、科学研究等。追求“通用性”或是特定目的都是可行的，但不同的目标选择会导致开发过程中的不同决策。

对于Debian而言，追求“通用性”意味着Debian不会根据软件的用途来打包。唯一真正的选择标准是软件是否自由，以及Debian是否能维护一个高质量的软件包。

章程、权力结构、治理模式

Debian是民主型开源组织之一，其具有明确且规范的决策流程，每年通过选举产生一位项目领导者。但项目领导者的权力受到严格限制，通常与领导职位相关的大部分权力都明确委托给其他人。

这种治理结构背后的历史背景是，早期Debian的几位领导者几乎拥有无限的独裁权，直到自行选择卸任。后来，由于一位项目领导者过度使用权力，引发了一场反叛，导致其被推翻，开始引入民主制度。作为其中的一部分，项目制定正式的章程[1]，明确项目的运作规则。

Debian之所以有当前的规则体系，是因为在其历史早期，较少的规则和较少的官僚主义并不能为其带来有效运作。

社会契约与Debian自由软件指南

20世纪90年代中期，在“开源”一词尚未被引入之前，“自由软件”的定义由自由软件基金会（Free Software Foundation）所确定，这其中又有许多待解释的地方。Debian希望有更明确的规则，于是提出《Debian自由软件指南》，并将其作为其社会契约的一部分。

社会契约是Debian对自身及全世界的承诺，阐述了Debian是什么以及做什么。DFSG（Debian Free Software Guidelines）也是其中的一部分，是Debian的基础文件，并有意使它在Debian章程中难以更改。

更为详细的规则使Debian可以接受何种内容更加明晰，并简化了相关讨论。当然，仍有许多需要深入探讨的问题。

后来，Debian自由软件指南（DFSG）成为了开源定义的基础。

自成一体

Debian坚持自成一体的原则。凡是由Debian打包的软件，必须仅使用Debian的依赖项来构建（编译）。此外，Debian中的所有组件都必须由Debian来构建，这会造成大量的额外工作。例如，当前的编程语言工具通常假定它可以在构建时从在线资源库中下载依赖，但这对于Debian来说是不被接受的。

主要原因是，依赖项在以后可能会变得不可用。Debian无法控制第三方软件包的仓库，如果某个软件包或是连整个仓库都消失，Debian就无法重建该软件包。Debian需要重建软件包以升级到新的编译器、修复安全问题、移植到新的体系架构，或者仅仅为了对打包的软件进行某些更改，包括修复漏洞。

如果Debian不是自给自足的，那么当需要发布紧急安全修复时，它就会受制于数以万计的软件包及其所有依赖包。这对Debian来说是不可接受的，因此，Debian选择将所有依赖包都打包了。

当然，对于Debian来说，意味着需要做大量的工作。

无捆绑库

Debian避免使用与软件包捆绑在一起的库副本或其他依赖项。许多上游项目发现捆绑或“供应商”依赖关系更容易，但对Debian而言，这意味着一些流行库就会存多个副本。当需要修复此类库中的安全问题或其他严重问题时，必须找到所有副本，逐一修复。这是一项繁重的工作，而且如果安全问题十分紧急，这样做会浪费宝贵的时间。

举个例子：zlib被大量项目使用。就其性质而言，它需要处理的数据可能是包含了恶意内容，用来利用库里的某个漏洞，这种情况确实发生过。有一次，Debian在其存档文件中发现了数十个捆绑的zlib副本的包，花费了大量精力确保Debian中的软件包只用了打包版本的zlib。因此，Debian选择在打包软件时，在紧急情况出现之前，提前做好工作，确保Debian中的软件包只使用Debian中打包的库的版本。

这并不总能得到上游开发者的喜欢，他们更倾向于只与他们捆绑的库版本打交道，这也是他们验证与自己软件兼容的版本，这有时会导致与Debian产生摩擦。

成员流程

鉴于Debian操作系统的规模和复杂性，以及其受欢迎程度，项目需要信任它的成员，尤其是要信任上传新软件包的人。由于20世纪90年代Linux的技术限制，每个Debian软件包在安装过程中都有完全的root 访问权限。换句话说，每位Debian开发者都有可能成为任何一台运行Debian机器的root用户。考虑到数千万台机器运行着Debian，意味着潜在的高权限带来的威胁。

Debian通过多种方式审核新成员。理想情况下，每位新成员都有足够长的时间参与Debian开发社区，被其他人所熟知，并在社区内建立了信任。

对于那些想要加入Debian的人来说，这个过程可能相当令人沮丧，尤其是那些习惯小型开源项目的人。

版本代号

Debian给每个主版本都分配了一个代号，其初衷是为了降低镜像Debian软件包归档的成

本。

20世纪90年代中期，在Debian1.0即将发布时，并未计划使用代号。相反，每个版本都有一个以版本命名目录的归档。由于开发新版本需要一段时间，所以就提前创建了“1.0”目录。很不幸，在Debian真正开发完成1.0之前，一家CD-ROM出版商过早的批量生产了他们标记为1.0的光盘，这意味着获取Debian 1.0 CD-ROM的人并未得到真正的1.0版本。

为了防止类似情况再次发生，一个显而易见的解决方案是把准备发布的内容放到名为“1.0-not-released”的目录中，发布完成后再把目录重命名为“1.0”。但是，当更改了目录名时，所有镜像都必须重新下载该版本。考虑到Debian的庞大规模（数百个软件包！数十兆字节！），这样做的成本很高。因此，Debian选择使用代号。

后来，“pool”结构被添加到Debian归档中。这样，所有版本的文件都位于同一个目录树中，元数据文件指定哪些文件属于各个版本，这使得镜像更容易。也许现在可以放弃代号，换成版本号，但我不知道Debian是否会对此感兴趣。

变化缓慢

正如前文所述，Debian的规模是庞大的，其庞大程度难以言喻，已经完全超出了小型的范畴。

大型船只停靠缓慢，大型项目也变化缓慢。Debian中任何影响到大部分软件包的变化都可能需要数百名志愿者来完成，这种变化不会迅速发生。

而有时，只需少数人就能完成工作，Debian有相应的流程来实现这一点。举例来说，如果上传了新版本的GNUC编译器，那么查找其他软件包需要做哪些修正工作，通常只需要少数人就能完成。修改需要时间，这需要达成共识，就需要广泛的讨论，而讨论需要时间，并且很少能够被简化或加速。

这也意味着Debian的开发者在技术决策上往往比较保守，他们通常更倾向于不需要大规模做更改的解决方案。

译者/Translators：

赵海玲Hailing ZHAO，开放原子开源基金会行业研究员

原文链接：https://blog.liw.fi/posts/2023/debian-reasons/

论文标题： Open source software and global entrepreneurship

论文摘要

这篇论文是首次研究开源软件（OSS）与全球创业之间的关系。本研究通过衡量国家在GitHub OSS平台上的参与度是否会影响创新企业的创立，以及对哪种类型的企业产生影响。我们利用各国新企业创立和OSS参与度之间的差异来估计这些影响。我们提出了一种使用工具变量的方法，并且不能拒绝因果解释。研究发现，一个国家在GitHub上的参与度增加，会在随后的年份内，促使该国家新技术企业数量的增加。证据表明，这种关系是对国家禀赋的补充，而不是替代。除了创业活动增长的正向变化之外，我们还发现了一个变化的方向：OSS贡献导致的新企业更加使命感和全球化，且质量更高。综合来看，结果表明，尽管需要人力资本前提，OSS可以提高创业活动。最后，我们考虑了鼓励OSS作为刺激创业增长政策的含义。

作者简介

Frank Nagle是哈佛商学院战略部门的助理教授。Nagle教授研究竞争对手如何在合作创造核心技术的同时，还能在建立在核心技术之上的产品和服务方面展开竞争。他的研究属于工作的未来、IT经济学和数字化转型等更广泛的范畴，并考虑技术如何削弱企业边界。他的工作经常涉及众包、免费数字产品、网络安全以及从非结构化大数据中生成战略预测等领域。他的工作利用从在线社交网络、开源软件库、金融市场信息和企业IT使用调查中获得的大型数据集，Nagle教授的研究成果已发表或即将发表在《管理科学》、《组织科学》、《战略管理杂志》、《研究政策》和《战略管理评论》等学术期刊，以及《哈佛商业评论》、《麻省理工学院斯隆管理评论》和布鲁金斯学会TechStream等面向实践者的刊物上。他曾获得AOM、NBER、SMS、INFORMS、EURAM、斯隆基金会和Linux基金会的奖励和资助。他是HBS/Linux基金会核心基础设施计划的联合主任。在哈佛商学院，他是哈佛数字、数据与设计（D^3）研究所、未来工作管理项目以及

哈佛创新科学实验室（LISH）的教员。

Nagle教授是Nexleaf Analytics和Alphamatician的顾问委员会成员，并为其他大数据分析初创公司提供咨询。他目前为经济合作与发展组织（OECD）创新与技术政策工作组提供咨询，并且是欧盟委员会/欧洲开放论坛开源对欧洲技术独立性、竞争力和创新的影响专家委员会成员。他曾为世界银行、美国财政部、社会保障局以及技术、国防和能源领域的多家公司提供咨询服务。他目前是对外关系委员会的任期成员。

推荐感悟

Frank Nagle教授近几年发表的论文，尤其是关于开源的，是颇具原创性的洞察，其在早在2014年，和著名的互联网经济研究专家Shane Greenstein共同发表的关于Apache的经济贡献就堪称人间清醒，后来更是在2019年发表了开源中关键的人力资源文章，今年又和Linux基金会研究部分发表关于安全对于开源的影响。本篇仍然具有开创性，究竟要不要支持开源，对于经济到底有何作用，OpenUK的那个GDP的影响值并不具备说服力，那么和创业的关系出发，非因果但相关，也是给我们当下以众多支持开源的决策者们一些启发。

论文下载：https://www.hbs.edu/faculty/Pages/item.aspx?num=63964

论文标题：《SOME SIMPLE ECONOMICS OF OPEN SOURCE》（《开源简易经济学》）

作者简介

Josh Lerner是哈佛商学院雅各布·希夫（Schiff）教授。他毕业于耶鲁大学，主修物理学和技术史。曾在布鲁金斯学会、芝加哥的一个公私合作工作组和国会山就技术创新和公共政策问题工作过数年。随后，他获得了哈佛大学经济系博士学位。

让·梯若尔（Jean Tirole）教授，在2014年获得了诺贝尔经济学奖，是世界著名的经济学大师，世界经济学家排名第二。现担任法国图卢兹大学产业经济研究所科研所长，同时在巴黎大学、麻省理工学院担任兼职教授，并先后在哈佛大学、斯坦福大学担任客座教授。1984年担任计量经济学（Econometrica）杂志副主编。同时还是普纳思经济管理研究院学术委员。2014年诺贝尔经济学奖被颁发给法国经济学家让·梯若尔，以表彰其“对市场力量和监管的分析”。

论文概要

人们对开源软件开发的兴趣激增，这涉及许多不同地点的开发人员和组织共享代码以开发和重新开发程序。对于经济学家来说，从事开源项目的个人程序员和商业公司的行为最初是令人吃惊的。本文对开源软件的经济性进行了初步探讨。本文强调了劳动经济学，特别是关于“职业问题”的文献和产业组织理论在多大程度上可以解释这些项目的许多特征。其实，开源软件相关的有趣研究问题还有很多尚待挖掘。

推荐语

·开发者为何参与开源项目?

·为什么有些项目能够脱颖而出?

·商业公司如何在开源运动中寻找利益?

这可能是很多人都在思考的问题，也在观察中验证自己的想法，每个旁观者都可能会给出不同的解释，但是亲历者则会给出肯定的答案 ~ 也就是说身处其中和旁观者是完全不同的。本论文所探究的问题，或许没有符合各位看官的意见，但是确实是众多多样性答案中的一部分。开源世界无论你是否参与它都在哪里存在着，你要么加入，要么享受其成果，唯一无法做到的就是忽略。

论文下载：https://www.jstor.org/stable/3569837

论文标题：《Understanding the Archived Projects on GitHub》

中文翻译：《GitHub上的归档项目探索》

作者介绍：夏小雅，华东师范大学在读博士；赵生宇，同济大学在读博士。

论文观点与摘要

GitHub上的开源软件（OSS）正在持续增长，尤其是在项目创建方面的快速增长。随着开放源码软件的发展，许多项目面临衰退，其中一些项目不可避免地降级为未维护状态并被所有者存档。了解已弃用的项目有助于加深对OSS维护和演进的认识。本文描述了对361个已存档的且曾经流行过的GitHub上的开源项目的研究。通过阅读代码仓库自述文件并向项目维护人员发送调查，我们发现软件代码库由于变迁、演变或未维护而被存档。我们提供了一组16个原因和10个实践来描述这些项目存档的原因和方式。作者通过拟合OSS开发活动生命周期曲线来进一步揭示其提交历史曲线。作者还确认了影响开源项目可持续性的总线因素风险的重要性。存档软件仓库是代码仓库弃用的明确标志。通过提供归档项目的原因（原因）、策略（如何）和生命周期模式（内容），为我们带来了促进开源项目和整个生态系统的健康和可持续性的影响和实践。

适兕感慨

由于人稀缺的注意力，往往会删去和简化一个事物的过程，开源项目千千万，能够被识别和认可的往往是那些成功的。然而，不为人知的，再也没有机会走到人们视野的项目则是大多数，当然他们或许是大多数项目的命运，正如那些每天都在不断消亡的创业公司，我们也应该将适当的注意力转移到这些项目上，他们犯了什么错误？或者说他们做了什么，以至于走着走着就消失了。我们是不是应该引以为戒？还是冷眼旁观？

论文下载：https://ieeexplore.ieee.org/document/10123670

2023年人工智能与开源界的风云变幻[译]

杨东杰推荐理由：

观察人工智能科技和产业发展中，开源力量的崛起和挑战和影响。

译文：https://baoyu.io/translations/ai/ai-and-open-source-in-2023

Gitlab的远程文化

苏帅推荐理由：

GitLab作为一个全员远程的上市公司，他们的远程文化值得所有想找远程工作的人学习，堪称[远程工作手册]。

访问链接：https://handbook.gitlab.com/handbook/company/culture/all-remote/handbook-first/

两代人沙漠种树的”智慧”

荆雯推荐理由：

大自然的智慧，在开源领域同样适用。

访问链接：https://mp.weixin.qq.com/s/xVUJ8LzReF7Ed2wsV3UmQQ

【开源项目】IP-Adapter

苏帅推荐理由：

这个腾讯AI实验室开源的IP-Adapter的思路挺不错的，在预训练的文本到图像扩散模型和附加结构控制器上进行各种图像合成，由于只使用文本的方式去生成图片涉及到能力很复杂，通过「一图胜千言」的方式省去了不少成本。

访问链接：https://ip-adapter.github.io/

开源项目Maintainer的标准

苏帅推荐理由：

对于刚起步的开源项目而言，这些眼花缭乱的标准背后，其实是一个大致相同的对项目维护者的标准。对于想要深入参与开源社群的人来说，理解了项目维护者的标准，也就明白该做些什么以成为一名维护者了。本文主要对这个标准的不同层面进行讨论，顺带对比上面这些经过演变的不同版本。

访问链接：https://mp.weixin.qq.com/s/y8ewE2blF3wa2hmQJvLu5g

开源即责任

tianchang推荐理由：

因为GitHub的盛行，“开源”成为了当下开发者非常“政治正确”的一个行为。每天在掘金里，我都会看到很多用户写文章说自己开源了这个、开源了那个，同时每年GitHub年度总结里不断飙涨的Repo数据和Commit数据好像昭示着开源生态和文化已经深入人心。然而，事实并非如此，甚至大家对于开源的理解，本身就是让人心寒的。就好像，我们生活在如此便捷的互联网时代中，却并未因此而创造更多。开发是一群有很强判断能力的人，我希望借由此文章帮助大家稍微多理解一些开源。

访问链接：https://juejin.cn/post/6844903746946744333

接受中国后来者在国际ICT标准化中的技术贡献——起源、经验和协作的作用

杨东杰推荐理由：

成功的开源项目可以视做事实标准，而这篇论文主要研究中国在标准竞争重地通信标准的参与和成果情况，得出的结论非常值得国内发起的开源项目参考。

原文链接：https://www.sciencedirect.com/science/article/pii/S00487333

22001779

23岁博士生帮助Firefox修复22年历史的bug

赵海玲推荐理由：

23岁博士生帮助Firefox修复22年历史的bug，在开源的世界里，就像进入一个丛林，往前走啊走，就会遇到很多不同的惊喜。很好奇，开发者第一次开源项目贡献时，会不会有些有趣的经历或是感受，感觉可以征集下。

原文链接：https://arstechnica.com/gadgets/2023/10/22-year-old-firefox-tooltip-bug-fixed-in-a-few-lines-offering-hope-to-us-all/

TO DO Group发布OSPO通讯10月

适兕推荐理由：

最新的研究揭示了2023年 OSPO 发展状况：年度 OSPO 研究调研了开源办公室及跨部门的开源倡议组织的普及率和结果，包括关键收益、提供的价值和未来挑战。

原文链接：https://www.linuxfoundation.org/research/ospo-2023

操作系统革命（纪录片）

杨东杰推荐理由：

鲜活的方式了解开源早期历史。

访问链接：https:/www.bilibili.com/video/BV1gx411Q79H/?share_source=copy_web&vd_source=b4377f881b59b99fbe1c31ab6a06fbee)

RSIC-V基金会主席最新发声：开源是全球的共同体

适兕推荐理由：

针对一些美国政客的无中生有，RSIC-V 主席的及时声明。开源不应被政治化！

原文链接：https://riscv.org/blog/2023/10/risc-v-an-open-standard-backed-by-a-global-community-to-enable-open-computing-for-all/

开源语言大模型的正确姿势

杨东杰推荐理由：

开源大模型的未来值得关注，建议配合另一篇《为什么开源大模型终将胜出？》阅读。

本文着眼于第一点：如果维持现状，那么开源语言大模型公司能否缩小与谷歌或OpenAI等巨头之间的差距？本文作者Nathan Lambert是伯克利人工智能博士和Hugging Face的机器学习科学家。

原文链接：https://mp.weixin.qq.com/s/ob96utZK_C1gCOGrQ78lJw

最高法公开一起开源知识产权案例判决：开源软件著作权侵权纠纷原告主体资格的认定

杨东杰推荐理由：

开源知产的案例值得关注。

原文链接：https://mp.weixin.qq.com/s/HqbOe61Nfr8_3cyyZFkYyg

基础软件到底需要什么样的自主可控？

杨东杰推荐理由：

开源与自主可控是什么关系？非常支持这篇文章的观点：

积极参与全球开源软件产业供应链治理，提高国内软件公司与团队在全球顶级基础软件开源项目中的话语权，培养具有全球视野与先进研发能力的技术团队。应当停止低水平重复的“国产操作系统/数据库内核分叉”，着力打造具有国际影响力的服务与软件发行版。

原文链接：https://mp.weixin.qq.com/s/YZWclUHaoK35DAwXB5Ta0g

人工智能国际领先机构OpenAI创新管理模式及对中国的启示

苏帅推荐理由：

以人工智能领域的国际领先机构OpenAI为例，探究其创新管理模式及对中国的启示。OpenAI通过打造以大模型为核心的创新引擎，依靠场景、人才、生态、科技金融与安全治理等5个方面的管理创新，建构了以AI大模型为基石、青年人才挑大梁、海量场景驱动的开放型创新生态系统，实现科技—金融—产业场景的良性循环，进而从后发企业快速追赶超越成为全球人工智能领军企业。OpenAI的实践为我国政产学研各方主体深入把握新一代人工智能发展规律和创新模式，加快通用人工智能创新和产业化，培育世界一流企业，打造中国式现代化新引擎等提供了重要参考。

原文链接：https://mp.weixin.qq.com/s/NtU5RlmnQKNuUzJxztmfxQ

《From Project to Profit：How to Build a Business Around Your Open Source Project》

《从项目到营利：如何围绕开源项目构建业务》（暂译）

内容概要

当你考虑开源和商业时，很容易陷入一种错误的二分法。开源是一种无私的合作，还是一种商业行为？答案是……是的！

有些开源项目是利他主义，是真正无私的献给世界的礼物，或者是建立简历证书的一种方式。但有些开源项目也可以成为新型企业的跳板。商业开放源码软件（COSS）企业具有资本效益，可以利用开发人员的信誉建立品牌资本。

从项目到营利是一本手册，帮助正在建立COSS企业的开发者找到从开源项目到可持续企业的道路。

作者介绍

希瑟·米克（Heather Meeker）既是专注于技术交易的律师事务所Tech Law Partners.LLP的合伙人，同时也是专注于商业开源开发的早期风险投资基金OSS资本的合伙人。

希瑟·米克长期为技术客户提供知识产权方面的咨询服务，是国际知名的开源软件许可专家。2019年，米克作为上榜律师，与Salesforce、Stripe及微软的首席执行官们一起，被美国商业内幕网站评为改变科技行业经营方式的十大人物。

希瑟·米克是美国法律研究所《软件合同法原则》和《法律重述-版权》项目咨询委员会的成员，还是IEEE-ISTO的董事会成员，著有《商业开源》。

推荐短文

在过去的四十年，商业软件以闭源和售卖许可的模式赢得了广泛的市场，以至于形成了一种以为商业软件只有这种模式的错觉。其实不然，在这个庞大的市场中，如果你仔细识别的话，商业软件以开源和售卖服务等方式占据了一隅，尽管份额较小，但并不是没有可能。这个世界上没有什么绝对的事情，软件的开源与闭源不过是同一事物的两种形态，他们如何从消费者/使用者手里获得该有的回报，这是一件关于交换、秩序和技巧的商业业务，所以，我们应该绕开关于爱、无私奉献和一刀切、二分法之类的说辞，应该找到能够解决人们问题的真实意图。在中国，以开源为特点的软件，市场仍然是巨大的，只是我们可能需要在业务上下一些功夫，Heather Meeker 的这本新书可以给我们一些参考价值。

关于第二期的主题——“开源基金会”

遍历历史上的开源软件基金会发展历程，所起到的作用，以及需要做什么？

例如：

开源基金会承载的是什么？

国内外开源基金会发展路径对比？

在中国慈善法的背景下，如何更好的发展开源基金会？

……

又比如：

企业为什么要做开源的决策？

真正好的开源项目/开源社区是什么样子？

……

或者再比如：

我们可能要策划一场直播活动……

快来说说，你最想听到的内容吧：

https://atomgit.com/OpenAtomFoundation/Global-Open-Source-Insights/discussions

“大家的洞察 更好的开源”《开源态势洞察仓库》地址：

https://atomgit.com/OpenAtomFoundation/Global-Open-Source-Insights，诚邀共建我们的“开源项目”