深度信息技术（精品）专辑
第八期

- 点评EDA电子设计自动化
- 开源治理与创新
- 建设供应链保障供应链安全
- 快速增长的开源供应链风险
- 打造开源软件供应链重大基础设施
- 简析开源相关的法律风险
- 人工智能（脑机接口）动态

中国开源软件推进联盟
China OSS Promotion Union

目 录

[1] 本刊编者：陈伟、鞠东颖。

电子设计自动化（EDA）

点评 EDA 电子设计自动化

陆首群

在 4 月 19 日 COPU 例会上讨论了解决“缺心少魂”的问题，而且把“工业软件”纳入这个解决的范畴。

在 COPU 例会会议纪要中，曾讨论将工业软件分为广义和狭义的概念：广义指如 PLM / ERP / CRM / MES / CAX，狭义指 EDA（或稍扩大指 CAD、CAE、EDA），对国内威胁最大的是狭义的 EDA，因为它主要由美国垄断（Synopsys，Cadence，MenterGraphics），占全球市场 64%，中国市场 95%。美国商务部长扬言要对中国断供的也是指 EDA（中科院计算所包云岗副所长会晤中芯国际时讨论并给我们反馈信息指的也是 EDA）。

在这里推荐大家阅读 COPU 刘澎副主席兼秘书长转载搜狐网 / 集微网的一篇文章：“筚路蓝缕、砥砺前行国产新兴 EDA 公司最全盘点”（该文编者按指出，美国三大公司垄断 EDA 技术掌控中国市场 85%）。

文中列出国产新兴 EDA 公司 27 家，其中核心企业约 14-15 家，与美国三大企业有关联的约 5 家（如全芯智造为合资企业，凯鼎电子为其旗下企业，阿卡思主要人员来自三大企业，深维科技是 Cadence、IBM、微软与中资企业合资的企业，

图元软件签协议采用 Cadence EDA 软件），至于涉及知识产权的还有几家，另外还有一些由硅谷海归、全球高端人才或港资创办的 EDA 企业，国内主要的 EDA 公司如国微集团、中科院微电子所、华为九天、九同方微电子、芯愿景、芯和半导体等。

初步结论是:国内新兴 EDA 公司基本上能承接 EDA 任务，如果按美方 2019 年 5 月制定的标准：不准中方企业采用美国技术，或追究是否涉及知识产权问题，则 EDA 短板就可能突出（这时在芯片领域去美化任务相当艰巨），即使如此，在今天国内完成 EDA 任务时还不至引发崩溃（当即在全国要作好布局）。

请大家再看一下 4 月 23 日刊载于今日“头条”的北河科技“美芯巨头被调查后，中科院做出官宣，华为机会来了？”的文章（该文著作方声明：“本文原创，禁止抄袭，违者必究”，我们声明并不抄袭其文章写作论文，只是引用其公开发表的材料，在内部讨论一些问题）。

该文谈到，美国商务部与商务部工业安全局分别两次调查美企新思科技（Synopsys），怀疑其向华为海思提供芯片设计和软件，或涉嫌与某些中国实体交易，结果查无实据被迫收场，实属敲山震虎！

今年 4 月下旬，中科院微电子所 EDA 中心在官网上宣布：“基于高性能计算的集成电路电子设计自动化（EDA）平台”

（项目）顺利通过了项目综合绩效评价。

该项目基于国产 EDA 工具先进工艺设计流程，对 EDA 工具的功能和性能进行对比和测试，并对其可兼容性、易用及稳定性等进行验证，形成规范的 EDA 工具评测报告。通过一系列的测试和验证,促进国产 EDA 工具的改进、更新和完善。

本项目的四个研究重点：

1、三维纳米级电路可制造性设计方法及 EDA 技术（满足大型纳米芯片 DFM 技术需求；

2、高频电磁场分析及仿真技术的 EDA 测试技术；

3、亚阈值低功耗设计方法及 EDA 技术；

4、支持千万门级的高速并行 SPICE 后仿真技术（性能超过主流工具 4-6 倍）。

芯恩半导体、中微亿芯、飞腾、海信等企业都已开始应用部分成果。

谈一下华为的机会：

随着国产 EDA 技术的诞生,华为也在加紧 EDA 软件布局，华为旗下哈勃科技投资公司近年对九同微电子（华为入股 15%）、上海阿卡思微电子、立芯软件（华为持股 20%）、无锡飞谱电子进行投资。

国产 EDA 崛起进行时

本刊编者[2]

2008 年起，EDA 再次获得了国家的鼓励和支持，被列入《国家中长期科学和技术发展规划纲要（2006-2020）》所确定的十六个重大专项之一。

2008 年 4 月，国家“核高基”（核心电子器件、高端通用芯片及基础软件产品）重大科技专项正式进入实施阶段。华大九天、芯愿景、概伦电子等第一批国产 EDA 企业相继成立并被重点扶持。

华大九天的 EDA 部门独立出来专注于 EDA 软件的研发。将突破口选在还未被巨头们重视的液晶领域，华大九天目前是全球唯一一个能够提供全流程 FPD（平板）设计解决方案的供应商。

概伦电子于核高基项目立项阶段同期成立，一直致力于提升先进半导体工艺下高端芯片设计工具的效能。2019 年收购 EDA 公司博达微科技，成为国内第一个有规模的 EDA 企业整合。

自 2018 年以来，受中美贸易摩擦影响，国内高新技术企业如华为、中兴等陆续受到美国制裁，芯片断供、EDA 软件

[2] 本刊编者：陈伟、鞠东颖。

停售等惩罚性措施导致相关企业经营陷入停滞，但与此同时，国家层面也把对国内半导体产业的关注提升到新的高度。

只有把关键核心技术掌握在自己手中，才能从根本上保障国家经济安全、国防安全和其他安全。作为关键基础软件，EDA 国产化势在必行。国家先后出台了一系列针对 EDA 产业的扶持政策，以加速行业成长。2018 年以来的部分 EDA 产业扶持政策如下：

1、《关于集成电路生产企业所得税政策问题的通知》，2018 年 3 月；

2、（关于推动创新高质量发展打造“双创”升级版的意见），2018 年 9 月；

3、《加强“从 0 到 1”基础研究工作方案》，2020 年 1 月；

4、《新时期促进集成电路产业和软件产业高质量发展的若干政策》，2020 年 7 月；

5、《国家鼓励的集成电路设计、装备、材料、封装、测试企业条件》，2021 年 4 月。

特别是《新时期促进集成电路产业和软件产业高质量发展若干政策的通知》（8 号文）在财税、进出口、投融资、科研、人才、知识产权、市场应用、国际合作等八方面对半导体产业发展予以扶持。随着“8 号”文的发布实施，政策、资本对 EDA 领域的关注度愈加高涨。

在风口之下，又现出了一批新兴的EDA企业，并开始崭露头角。比如国产新兴EDA企业——合见工软，高效地发布了四款EDA产品，包括数字仿真器（UVS）、原型验证系统（UVAPS）、协同设计环境（UVI），以及电子设计数据管理平台（EDMPro）等。

（关于这些新兴企业的介绍，联盟陆主席在“点评 EDA电子设计自动化”一文也提到参看：“筚路蓝缕、砥砺前行国产新兴EDA公司最全盘点”一文。）

2021年有多起中国EDA企业 成功“IPO”的案例。6月21日华大九天创业板上市受理；6月25日概伦电子科创板上市受理；6月30日广立微创业板上市受理；8月24日国微思尔芯科创板上市受理。上述四家EDA公司IPO拟募资约57亿元。

以华大九天、国微集团、芯华章、广立微、概伦电子、芯和半导体、合见工软等企业为代表的国产EDA公司，厚积薄发快速提高技术实力，完善中国集成电路产业链，中国EDA企业在崛起的道路上高歌猛进！

开源治理与创新

开源治理与创新

Brian Behlendorf 在中国软件产业年会的演讲[3]

大家好，我是Brian Behlendorf，Linux基金会旗下开源软件安全基金会(OpenSSF)总经理。今天，非常感谢中国软件行业协会让我有机会与大家交流。在此，我借用一句名言“软件确实在吞噬世界”。软件早已成为每个国家社交媒体、通信系统，以及各种金融体系和政府流程的核心，甚至已经嵌入每一辆车、每一个设备，每一个门把手。

软件还涉及到各行各业，从主要供应链到教育、医疗等领域。软件的确无处不在，而开源软件的兴起是软件无处不在的主要驱动力之一，也是它的关键支柱之一。在某些方面，开源软件甚至比早期的专有软件起源更早。在计算机时代的某些时候，大型机总是会获得源代码，而你买来运行业务的计算机能按你的期望修改它的运行方式。

目前，根据估算和研究显示，大约 90%的软件平台或嵌入软件应用程序的开发使用了开源软件。并且开发者在使用的同时通过改进还给源代码赋能了 10%的额外价值，那么，

[3] 本文为 OpenSSF 基金会总经理 Brian Behlendorf 在中国软件行业协会主办的 2022 中国软件产业年会上主题演讲的中文翻译稿。

我们就需要思考，开源软件是怎么来的？从哪里来的？它的主要驱动力又是什么？开源软件治理正在不断向前发展，如何支持它，如何更快地推动它为我们创造更多价值，是未来治理开源软件的主要目标。

今天，我想重点谈谈两个关键的创新，分别是开源基金会的兴起和开源项目办公室的兴起。开源基金会的历史最早可追溯到19世纪80年代，第一个开源基金会名为“自由软件基金会”。创立之初，它的宗旨与微软、施乐以及一些主流公司截然不同。它倡导“软件免费”，这引发了一个“道德议题”，并引起了一些人的共鸣。但是对于希望在商业上使用该软件的人们来说，这是一个明显分歧。一些相关的企业开始在市场上出现。在此浪潮之上，自由软件基金会应运而生。自由软件基金会组织推广和帮助人们了解在新公共许可下编写和发布的代码的价值。

在 90 年代中期的1995 年，一个不同类型的开源基金会成立了，这就是 Apache 软件基金会，我参与了这个项目，并且在初创阶段发挥了不小的作用。

* Apache 软件基金会（也就是 Apache Software Foundation，简称为 ASF）是专门为运作一个开源软件项目的Apache 的团体提供支持的非盈利性组织。Apache基金会

创建之初的想法是，软件应该是一种公共产品，企业可以使用，个人也可以使用。无论任何使用原因，我们都应该齐心协力致力于创造这一共同的、共享的知识产权，以提高某种共同的能力。但我们每个人都应该能够允许通过软件去赚钱或者解决问题。

它主要基于个人、企业，是非正式角色，而非具体公司。来自各方的 Apache 软件基金会成员，都给予基金会一定赞助。基金会也会切实帮助企业更容易使用和理解这个软件。然后在 2001 年，也就是 Linux 内核的第一个版本发布 10 年之后，一个叫 Linux 标准库的组织成立了。开源实验室最终发展成了 Linux 基金会。

当时 Linux 操作系统开始受到大大小小的组织的关注，他们在超级碗上投放广告，宣传他们基于 Linux 所构建的产品，促使人们开始意识到需要一些基础设施来支持代码的开发。这也可以帮助管理使用这些代码的公司，因此 Apache 率先创建了标准化版本控制工具的使用。每个项目都有一张标准许可证和一组标准邮件列表。Linux 基金会在早期，主要专注于如何构建 Linux 内核，开发人员使用的构建系统是什么，以及如何实际管理内核和管理成千上万的贡献者。

然后，在第二个阶段，则主要关注如何管理 Linux 周围的商标，如何确保众多公司可以在平等的基础上，使用这些代码来构建产品和服务。随后又可以像所有企业一样相互竞争。Linux 基金会发现了这一点，它发现了如何建立一个企业支持模型，为一个中央办公室提供资金，帮助管理营销和开发者关系。而且，提供了协作基础设施、构建工具和围绕 Linux 操作系统的所有安全服务，这是一个重大进步。随着时间的推移，约在 2006、2007 年间，Linux 基金会意识到它为 Linux 操作系统和 Linux 内核所做的事情可以复制到其他软件领域。

今天，你可以看到 Linux 基金会项目在 Linux 基金会的护佑下专注于从 5G、物联网、边缘计算到汽车行业软件、能源市场软件、医疗保健乃至数百个其他项目（其中有一些较为低端）。但是像 Kubernetes 这样的项目，则是当前全球范围内主要的云计算平台。以及许多其他云原生技术都是在云原生技术基金会中的项目。总而言之，你可以看到数百个项目覆盖了这些开源项目中超过 10 亿行的代码。有 500 到 1000 名左右的开发人员积极参与其中，开始使用它的代码，并在源代码之上继续构建。

总的来说，所有这些项目公司带头合作，共同构建一些

东西，帮助所有公司推进他们的战略目标，围绕更好的软件的非常务实的需求，并共同努力实现这一目标，顺便说一句，Linux 基金会的成员包括华为、腾讯、阿里云、蚂蚁金服、字节跳动，还有更多来自中国和亚太地区其他地区的组织和公司参与到了基金会的众多项目中来。Linux 基金会在确保开源代码的全球可用性方面发挥了关键作用。我们有很多项目来自于这些公司和中国的许多其他公司以及他们的开发人员。

我认为，这类基金会是帮助开源项目在这类关键基础设施中发挥作用，对部署它们的企业做出响应的关键。向政府解释了开源项目的起源以及发展，进一步帮助了开源软件的全球化。从某种角度上说，这比任何一家公司所能带来的意义都大，这是非常令人鼓舞的事情。组织基础结构的第二部分，我想说的是开源项目办公室的兴起。

开源项目办公室简称为 OSPO，它通常是商业组织的一部分，甚至是政府机构或大学的一部分。他们负责弄清楚如何协调组织使用开源代码并将其贡献给开源社区。一些全球知名公司，比如沃尔玛、西门子，当然，还有 IBM、谷歌和微软，建立这样的办公室是为了能够更好地协调他们与开源社区之间的互动关系。除了核心软件金融服务公司、医疗保健

公司，还有很多组织都建立了开源项目办公室。通常，开源项目办公室是由技术人员和程序员组成的，他们了解开源代码的前景和开发方法。通常还会有来自市场营销或产品开发部门的人员加入其中，他们确保了如何能够改进开源代码。最后还有律师，因为律师喜欢确保版权得到遵守，商标得到遵守，以及每个人在使用和回馈开源时都能受到保护。

这些办公室真的可以推进标准化，或者说是，什么类型的开源项目可以在企业内部使用。我认为，这涉及到一些问题，比如哪些许可证是允许的，也许 Apache 许可证是允许的，但不包括 GPL，例如 GPLv3。它还可以帮助那些开发人员找出开放源代码包的不同选项，以解决特定的问题，哪一个是值得标准化的，哪一个是值得协调的，当它真的通过时。很多人去使用相同的代码，你得到了开源开发的积极方面，或者你让很多用户成为贡献者的子集，成为主要开发人员。我想说，其实我们在开源社区中可能有太多的代码，但是没有足够的软件开发人员，所以我们应该更加专注于分类出什么是真正领先的产品和项目。我认为，需要帮助公司和开发人员以及这些公司做出这个分类。他们还可以帮助公司选择更安全的产品方面发挥作用。这些软件包具有更好的历史记录，如果在公司外部或公司内部发现了属于安全问题的漏洞，事实上，这些 OSPO 可以以协调、有效的方式帮助上游项目管

理这些漏洞的披露。这是开源项目办公室所做的第二件大事，不仅仅是帮助控制开源代码进入组织。同时也是确保用户知道公司使用开源代码所做的任何改进、任何错误修复、任何功能的增加，任何功能添加，它们试图将上游推回开源项目，因为这对每个人都有帮助，它不仅可以帮助使用该代码的其他用户修复错误，甚至可以了解他们以前不知道的错误，事实上，它对每家公司都有帮助，因为当有更新版本的开源软件包时，会被自动修复，而无需进行第二次或第三次修复，所以一个好的开源项目办公室可以帮助上游，这项工作有助于确保开发人员在想要与上游开源社区互动时得到很好的支持，并且尽可能当它再次出现时，可以遵循更好的安全实践，需要处理安全更新或发现一种新的漏洞。

这正是我今天想谈的事情，这是 Linux 基金会的一项重大举措，也是我领导的项目。它被称为开源安全基金会，是一个专注于帮助整个开源社区获得更安全代码的项目，以帮助我们找到错误并更快的修复它们，以减少关键基础设施威胁类型的错误比如去年 12 月发生的 Log4j 错误，当我们发现了这个错误时，迅速在整个开源生态系统中修复了它们，并坦率地告知了所有开源代码用户。这是一个大约两年前开始的项目，现在已经得到了一些主要组织的承诺，包括华为和腾讯、闻泰科技、阿里云，我们非常渴望围绕开源安

全基金会在中国发展社区，与大多数开源项目不同，我们只创建一点点代码。而且，所提供的大部分内容都是关于如何编写更安全的开放源代码的教育材料。

我们有一个叫做“最佳实践徽章”的东西，它是开放源代码项目的检查清单，以确保他们遵循所有最佳安全实践在那里，可以更好地运行开源项目管理。还有一个名为 Security Scorecard（安全记分卡） 的自动化工具包，用于评估 Git Hub 存储库或任何其他代码存储库，并寻找良好的安全实践，例如，在你的单元测试中使用模糊测试或依赖待定，以确保你的应用程序中的依赖性代码固定到特订版本中，所以新版本即使出现了一些破损，你也不会出现问题。

这不会给你带来问题。因此，安全记分卡是一种尝试将其自动化的方式。总的来说，OpenSSF 正在进行很多升级来帮助用户更好的使用软件，为了帮助开源开发人员做出更明智的决定，比如在哪些平台上构建，哪些组件可以选择，并且在过程中，也希望推动那些希望在这些不同指标上取得更好成绩的开源项目，从而更受欢迎。这也可以帮助正在部署开源代码的企业去考虑他们在使用一个包而不是另一个包时所承担的风险，因为不是所有的开源软件都是一样的，不是所有的项目都以相同的方式运行，并不是所有的项目都具

有相同的成熟度在构建软件时要遵守纪律，我们希望提供一整套工具，并且实际上确实提供的是一整套工具和基础设施，来推动开源更加安全的使用，并推动一系列激励措施来改进该基线。

另一个项目的例子，Sigstore，它主要围绕检查和能够签名，软件工件通过软件供应链验证它的真实性，你知道开发人员的产品就不会受到中间人的攻击，并且能够对从最初的开发人员到现在部署的人员的所有过程进行审核。该标准和其他标准是我们所做工作的重要组成部分，他们的软件有助于支持 Sigstore 周围被称为 SLSA 的东西，OpenSSF 上发生的许多事情都说明了保护开源软件供应链的安全很重要，因为我们认为，软件世界的大部分内容都是建立在开源代码之上的，这有助于真正为整个软件行业建立供应链。所以鼓励大家来看看 openssf.org，看看我们正在构建什么，我们也非常渴望在此代码之上帮助构建中国社区。

下面，我来谈谈对中国公司和大学的一些建议，这些都是负责处理开源代码的技术和技术政策的组织。我认为每个大中型企业都应该建立一个开源项目办公室，它非常有价值，能让你更有效率的使用开源代码，我认为每个组织都应该要求他们的开发人员更多地关注并且重用现有的开源代码重

建一些东西总是有诱惑力的。当你看一个代码包只包含了一半的所需代码，就可以基于这个包继续去构建，或者做一些完全不一样的事情。

你可以利用这个包，而无需整个从头去写。这种重新构造代码，对于在每一行代码上获得更多关注并使其更加安全是非常重要的，因此你所做的这些，其本质是推动了重构和公共开源世界协作文化。如果你考虑在上游贡献修改，就去做吧，就像你使用开源代码一样工作，众多的代码贡献者修改它、改进它、增强它，确保它满足需求的同时还尽可能地把它们推向上游，让每个人都能从这些改进中受益。

无论你来自哪个行业，我都建议你在那个行业做开源项目，比如汽车、医疗保健或制药，金融和其它许多行业都在 Linux 基金会，甚至更多。无论是一家公司或是一个组织，关注你所在领域的主要开源项目，都是会有回报的。因此，在适当的时候，你可以开始使用该代码并从中受益，并避免重新发明已经成为惯例的东西。

最后，请大家到 openssf.org 中去看看我们在开源安全基金会所做的工作，学习如何使你编写的代码和你使用的代码尽可能的安全。非常感谢这次能有和你们交流的机会，我

也期待着有一天能在中国或其他地方再次与你们相见。非常感谢大家的聆听！

LF 和 OpenSSF 启动开源软件保护计划

本刊编者[4]

开源安全基金会（OpenSSF）和 Linux 基金会（LF）于 2022 年 5 月 12 日在华盛顿特区举行的第二次开源软件安全峰会上宣布启动 1.5 亿美元的开源软件保护计划，以修复十个主要的开源安全问题。

亚马逊、爱立信、Google、英特尔、微软和 VMWare 已经认捐了 3000 万美元，更多的厂商已经开始行动。

以下是开源产业致力于实现的十个目标：

1） 安全教育：向所有人提供基线安全软件开发教育和认证。

2） 风险评估：为前 10000 个（或更多）开放源码软件组件建立一个公共的、供应商中立的、基于客观计量的风险评估仪表板。

3） 数字签名：加快软件发布中数字签名的采用。

4） 内存安全：通过替换非内存安全的语言，消除许多漏洞的根源。

[4] 本刊编者：陈伟、鞠东颖。

5） 事故响应：建立 OpenSSF 开源安全事件响应小组，安全专家可以在应对漏洞的关键时刻介入，协助开源项目。

6） 扫描技术：通过先进的安全工具和专家指导，加速维护者和专家对新漏洞的发现。

7） 代码审计：每年一次对多达 200 个最关键的开放源码软件组件进行第三方代码审查（以及任何必要的修复工作）。

8） 数据共享：协调全行业的数据共享，以改善有助于确定最关键的开放源码软件组件的研究。

9） 软件材料清单（SBOMs）：推动改进 SBOM 工具和培训的采用。

10）改进供应链：通过更好的供应链安全工具和最佳实践，加强 10 个最关键的开源软件构建系统、软件包管理器和分销系统。

联盟陆主席呼吁 COPU 联盟成员要抓紧学习、领会供应链开源组件的安全技术和策略，以便在与 LF、OpenSSF 讨论时有发言权，为政府提咨询，承担基础设施／供应链交办的任务。

开源安全和开源软件供应链

建设供应链保障供应链安全

（基于“两个循环”、“两个市场”解决我国供应链安全挑战）

陆首群

2021 年 11 月阿里云团队发现在美国供应链上存在一个 Log4j 巨大的漏洞(隐患),他们首先报送给 Apache 基金会，引起了国际开源界极大的关切。

为了保护国家关键基础设施（如能源、银行、国防、公共卫生和防疫等）的安全，消除其供应链中广泛使用的开源组件或应用程序中存在的漏洞造成的影响，Linux 基金会于 2021 年 12 月 23 日成立了其旗下的开源安全基金会（OpenSSF)，由 Apache 创始人（之一）的 Brian Behlendorf 担任 OpenSSF 的总经理，随即该基金会提出应对开源软件供应链安全挑战的关键举措。

Brian 在 OpenSSF 成立会上谈到，在美国供应链的开源组件（或开源软件包）中发现存在一个严重的漏洞 Apache Log4j，这将导致出现 Log4shell（命令行解示器）严重混乱（在行业内属于四级警报)，另据行业机构不完全统计，该漏洞影响 6W+流行开源软件,影响 70％以上企业线上业务系统，漏洞波及面、危害程度堪比 2017 年的让数百万台主机面临被勒索病毒攻击品风险的“永恒之蓝”漏洞。

这个事件引起了美国政府严重关切，2022 年 1 月 13 日在白宫举行供应链安全问题讨论会，邀请 Jim Zemlin（Linux 基金会执行董事）和 Brian Behlendorf 作报告（白宫官员和专家参加会议，并邀请美国社会部分专家名流与会），会上普遍赞同报告人对供应链安全问题的分析、结论和作出的对策建议。

OpenSSF 针对供应链安全挑战的对策建议如下：

1、建立一支安全维护团队，及时、持续排除开源组件（或开源软件包）中的漏洞；

2、定期进行安全扫描（开发 CI 工具），检查发现开源组件（或开源软件包）中存在的漏洞；

3、对关键代码进行安全审计；

4、使用测试框架（供项目使用，以测试特性及淘汰未充分使用的特性）；

5、移除已弃用或易受攻击的依赖项；

6、使用符合软件包数据交换标准（SPDX）的、取代物料表格式（SBOM）的开源代码，追踪依赖关系，使之更易发现修复漏洞；

7、对维护人员提出要求：熟悉供应链及开源组件的安全知识，维护开源组件内部去漏洞。

下面我们来讨论如何建设、修复或改造我国的供应链，并保障供应链安全？

建设我国供应链保障其安全，必须立足于我国“两个循环”、“两个市场”的国情背景。

在我们的讨论中，首先集中讨论我国关键基础设施（列哪几项），讨论与其配套的关键供应链及其安全问题。

其次我们讨论建设我国关键供应链的技术发展方向，即是否把数字化转型作为建设、改造关键供应链的方向？

如果逐步建设、改造以分布式、数字化、协同主体组成新型供应链，为什么要采用开源组件（开源软件包）的开源代码来构建？

开源代码应符合哪种数据交换标准？如何取代传统的物料表格？

采取什么措施来保障供应链的安全？

我国“两个市场”供应链有什么关联？

本国供应链安全与全球网络安全有什么关联？

现提出我国供应链安全对策的建议如下::

1、基于“两个循环”、“两个市场”的理论和实践，可防止有人破坏、断供现有的全球供应链，解决对我国供应链的安全挑战。

2、在关键基础设施中某些高端产品的供应链在我国可能是缺失的（或不能自主实现的），如缺失高端芯片产业中的高端光刻机，有人以此来卡我们的脖子，摧残供应链的全球化配置，这时我们要组织科技攻关，尽快自主完善建设对我

国可能缺失或断供的供应链。

3、建设新型的关键供应链，实行数字化转型是其发展方向，我们提出的“对策建议”应结合数字化转型的特点进行。

4、新型供应链采用开源技术，不但有利于向供应链的主配关系中自然地注入开源的“协同”粘性，更为了便于计算和数据交换，符合SPDX标准的开源组件代码将取代物料SBOM表格，以支持供应链顺利运作，我们提出“对策建议”是针对开源供应链进行的。

5、我国供应链的“安全对策”可依据上述思路、参照OpenSSF的“对策建议”进行。

快速增长的开源供应链风险

隆云滔、武延军、齐安信

软件供应链已经成为网络空间攻防对抗的焦点，直接影响关键基础设施和重要信息系统安全。软件的供应链安全问题由来已久，只是随着开源软件规模化应用，软件供应链愈发复杂多元，使开源软件供应链风险尤其突出。开源软件供应链，指的是开源软件按照依赖、组合等形成的供应关系网络。与传统供应链不同，开源软件供应链存在迭代周期短、模块数量多、生产线上化、供应全球化、仓储集中化、边际成本低等特点，这也让开源软件供应链暴露在更多风险之下。Sonatype 2021 年 12 月发布的《2021 年软件供应链状况报告（2021 state of the software supply chain)》指出，从 2015 年 2 月到 2019 年 6 月，记录了 216 次软件供应链攻击。从 2019 年 7 月到 2020 年 5 月，攻击次数增加到 929 次。然而，在过去的一年中，此类软件供应链袭击事件超过 12000 起，同比增长 650%。总体来看，开源供应链存在持续维护、安全漏洞、知识产权和人为断供等风险。

一、持续维护风险

当前，大量软件产品依赖开源软件进行构建，这些被依赖的开源软件位居供应链上游，对下游产品安全具有重要的

影响力。一旦这些上游开源软件由于某些原因不再进行维护，下游软件产品势必会受到影响。据奇安信代码安全实验室《2021 中国软件供应链安全分析报告》数据显示，主流开源软件包生态系统中不活跃的开源软件项目数量为 2347794 个，占比达到 61.6%。这表明大量的开源项目处于失去维护的风险中。

开源软件持续维护风险的另一个表现是被恶意破坏，faker.js 与 colors.js 开源库就是典型例子。2022 年 1 月 10 日，个人软件开发者 Marak Squires 将其个人创建的位于项目仓库 GitHub 和开源组件包 NPM 上的开源库 faker.js、colors.js 的代码清空。由于成千上万的用户依赖这些库，本次恶意更新导致所有相关项目受到影响。使用遭到破坏的版本，会导致应用程序无限输出乱码。据报道，其清空仓库的代码是因为缺乏资金和被别人滥用开源项目，并声称不希望自己的努力成果为国际巨头企业免费使用。

开源软件持续维护方面的另一个风险在于开源作者的付出与收益不相称。2022 年 1 月，开源项目 Apache PLC4X 的创建者 Christofer Dutz 在 GitHub 发文称，由于得不到任何形式的回报，他将停止对 PLC4X 的企业用户提供免费的社区咨询，若后续仍无企业资助项目则将停止项目维护和任何形式的支持。

二、安全漏洞风险

安全漏洞在流行开源项目中非常普遍。根据奇安信代码安全实验室《2021 中国软件供应链安全分析报告》,截至 2020 年底，CVE/NVD、CNNVD、CNVD 等公开漏洞库中共收录开源软件相关漏洞 41342 个，其中 5366 个为 2020 年度新增漏洞。而在奇安信代码安全实验室审计的 2557 个国内企业软件项目中，存在已知开源软件漏洞的项目有 2280 个，占比高达 89.2%；存在已知高危开源软件漏洞的项目有 2062 个，占比为 80.6%；存在已知超危开源软件漏洞的项目有 1802 个，占比为 70.5%。这些项目中，共检出 168604 个已知开源软件漏洞（涉及到 4166 个唯一 CVE 漏洞编号），平均每个软件项目存在 66 个已知开源软件漏洞，最多的软件项目存在 1200 个已知开源软件漏洞。而从漏洞的影响角度来看，最多的 Spring Framework 安全漏洞 CVE-2020-5421 影响了 44.3%的软件项目，多个漏洞影响了超过 30%的项目。一旦具有大规模用户基础的开源软件存在安全漏洞，势必会影响整个信息产业的安全。

开源软件安全漏洞方面最知名的案例莫过于 Apache Log4j2。2021 年 12 月，Apache Log4j2 被发现存在因递归解析触发远程代码执行的漏洞。Log4j2 作为一个基于 Java 的日志框架影响范围之广远超开发团队的预想，全球近一半企业因为该漏洞受到了黑客的试图攻击。该漏洞最早由阿里云一名研发工程师发现，由于阿里云未在第一时间按有关规定

向电信主管部门报告，未有效支撑工信部开展网络安全威胁和漏洞管理，被工信部处以暂停了网络安全威胁信息共享平台合作6个月的处罚。

软件供应链的每个环节都可能会引入安全风险从而遭受攻击，上游环节的安全问题会传递到下游环节并被放大。攻击者不再等待公开的漏洞披露来进行漏洞利用，而是主动将新漏洞注入为全球供应链提供支持的开源项目中，通过将攻击转移到“上游”，可以获得影响力和关键的时间优势，使恶意软件能够在整个供应链中传播，从而对“下游”用户进行更具扩展性的攻击。

三、知识产权风险

根据新思（Synopsys）公司《2021开源安全和风险分析报告》，2020 年的被审代码库中有 65%包含存在许可证冲突的开源代码。纵观存在许可证冲突的代码库，近四分之三与某个版本的“GNU通用公共许可证”存在冲突。26%的被审代码库使用了没有许可证或定制许可证的开源代码。使用定制开源代码许可证的代码库是否存在可能的 IP 和其他法律问题，需要评估后才能确定。例如，JSON许可证实质上是宽松型MIT许可证,只不过添加了“该款软件严禁用于恶意用途，仅限用于善意用途”的注释。许多热门项目的责任单位都因为许可证定义含糊不清而删除了使用 JSON 许可证的代码，

因为“善意用途”与“恶意用途”定义争议性极强，很难界定。

四、人为断供风险

跨国界平等的创新与协作本是开源世界最基础的行为准则。然而，美国政府、相关企业均认同美国出口管制条例适用于开源社区和开源软件。有关伊朗、俄罗斯开发人员因美国出口管制限制而被禁止使用 GitHub 开源平台的事件时有报道。最新的案例是，GitHub 再次明确会遵守政府提出的出口管制和贸易法规，包括严格限制俄罗斯获得其维持侵略性军事能力所需的技术，俄罗斯程序员或因为制裁而无法正常使用 GitHub。

需要引起重视的是，除了因美国法律要求“不得已”而为之的断供外，因政治立场、情感取向等非法律因素导致开源断供的行为也开始显现。2022 年 2 月俄乌爆发军事冲突以来,“制裁俄罗斯、声援乌克兰”已经成为西方社会新一轮“政治正确”运动，不断有开源厂商因政治立场或个人情感的因素宣布断供俄罗斯，如 SUSE 宣布暂停在俄罗斯的所有直接销售，RedHat 停止在俄罗斯和白俄罗斯的销售和服务，Docker 取消来自俄罗斯和白俄罗斯的订阅服务等等，粉碎了“开源无国界”的假象。这让世人看到开源倡导的“创新、开放、自由、共享、协调”理念，在“政治正确”面前不堪

一击。

除了直接断供外，还有舆论主张通过张贴标语表达政治倾向，越来越多的国际主流开源社区不得不在舆论的压力下做出表态，如 Node.js、React.js 等都曾在官网表明支持乌克兰的政治立场，不过后来都因引起网友的广泛关注和反应而最终删除相关观点。

为了应对供应链存在的安全问题，首先应整体考虑供应链上下游关系，明确开源软件供应链的各个环节组成。其次，应对软件供应链产品进行全生命周期安全保障，从上游开始一直到软件部署及运行，对各个环节进行安全评估。此外，应从开发者、开源社区、地区分布等多个维度进一步评估关键开源软件的维护性和演化能力，确保其在供应链中的可靠性。最终极的解决方案，则是在上游开源软件和开源社区的基础上，由具有社会公信力的机构，牵头打造开源软件供应链基础设施，形成公共服务能力，对千行百业提供高质量、可持续的开源软件供应。

构建健全的开源供应链生态，**一是注重培养开源软件供应链安全人才**。建设开源供应链安全运维团队，建立关键供应链所涉及的各行业、企业内部当然应成立一支高素质的维护团队。大力培养开源供应链安全管理、技术与战略人才，从战略、战术上给予重点培育培养。**二是构建开源供应链安**

全评估体系。扶持一批从事开源软件安全评估的创新企业，打造开源供应链的安全评估体系。从开发者个人、企业发展、开源组织、国家政策等五个维度构建开源供应链安全评估框架，制定开源供应链安全行为准则，实时监测国内开源供应链的重点事件。从战略政策层面，持续关注跟进开源软件、开源硬件供应链的国际形势。实时跟踪了解国际开源供应链的动态，特别是各国在开源供应链方面的政策举措及落地方案。**三是建立开源供应链安全实验室。**以信息产业安全发展为目标，以繁荣开源生态为导向，确保信息产业供应链安全。通过开源供应链安全实验室打通个人开发者、企业、政府管理部门三者之间的旋转门机制，鼓励企业的一线开源开发者到政府管理部门工作，同时允许政府管理人员到开源企业从事管理与战略工作。

打造开源软件供应链重大基础设施

武延军、吴敬征、武斌、赵琛

全球范围内，开源软件已经成为信息基础设施的核心要素，是构成操作系统、数据库，以及其他大型复杂基础软件和应用软件的核心“元器件”与“原材料”。能否为设备、系统、产业和行业提供高质量的、高可靠的、可持续演进的开源软件供应，关系到国内当前和未来 IT 科研、产品与生态的核心竞争力。然而，近年来，开源软件供应链风险事件频发，开源软件产业面临着不少根本问题。为了贯彻落实开源软件国家战略，实现开源软件的可靠供应，需打造核心基础设施支撑能力，评估、监控和消除开源软件存在的风险，推动我国开源软件产业走上高质量的发展道路。

一、 什么是开源软件供应链

随着软件规模越来越来大，软件项目之间同样存在着越来越明显的合作和供应关系，相应的也存在供应链的概念。例如，基础软件通常属于大型复杂软件，存在明显的供应链特征，而且比硬件更为复杂。一个典型的开源操作系统（如 Ubuntu、Android 等）是由数万个上游开源软件以及部分非开源软件组成的。这些上游开源软件被广泛复用，成为软件

世界的“原材料”和“元器件”。操作系统构建过程本质上就是对开源软件供应链的整合优化过程。我们把开源软件领域存在的这种供应链关系，称之为开源软件供应链[1]。开源软件供应链的一个非形式化定义表述如下。

开源软件供应链是一个实际业务系统在开发和运行过程中，涉及到的所有开源软件上游社区（Upstream）、源码包（Source Package）、二进制包（Binary）、包管理器（Package Manager）、存储仓库（Repository），以及开发者（Developer）和维护者（Maintainer）、社区（Community）、基金会（Foundation）等，按照依赖、组合、托管、指导等关系形成的供应链网络。

这是一个相对宽泛的定义，或者可以称之广义的开源软件供应链定义。相对的，狭义的开源软件供应链只涉及到开源软件本身（源码包或者二进制包）的依赖、组合等关系。

二、 开源软件供应链存在的风险

通常情况下，软件包管理工具可以看作狭义开源软件供应链定义下的一种管理工具，只解决一个操作系统发行版内部软件包之间的依赖关系。而广义开源软件供应链的情形下，则需要处理更为复杂的问题，可以划分为四个方面：知识产权风险、代码质量问题、漏洞传播风险以及持续维护风险。下面对这四方面的关键问题进行简要的讨论。

（1）知识产权风险

任何开源软件一定会有一个开源许可证。开源许可证标志着使用者可以在何种程度上使用以及改造、发布源代码。有一些许可证非常宽松,比如 MIT 许可证。当源代码被修改后，可以选择闭源，而且不必注明版权，当需要宣传软件的时候，还可以用源代码的项目名称进行促销背书。有一些许可证则非常严格，比如 GPL，当源代码被修改后，新的代码也必须要开源，同时必须也使用 GPL 许可证。

（2）软件质量问题

漏洞（Vulnerability，也被称为脆弱性或缺陷）广泛存在于每个软件之中。一些漏洞会引发广泛的恶劣影响甚至攻击行为，一些漏洞直到软件生命周期终结也不会被发现。同许可证问题一样，海量的软件包会带来大量的缺陷代码。使用者不可能对每一个软件包进行漏洞筛查。但这些带有漏洞的开源软件很有可能如同尘封多年的哑炮一样，不知道什么时候会毫无征兆的炸开，从而让整个业务系统宕机并蒙受损失。针对软件漏洞,目前有一些漏洞扫描工具,如 Vtopia、FOSSID，SONATYPE 等。这些软件通过整合上游社区发布的漏洞信息，以及主动扫描发现漏洞信息来做到提前预警。

（3）漏洞传播风险

当一个大型复杂软件发现新的漏洞时，必须有具体到个人的精准修复指示，才能提高漏洞修复的速度。对于公司维护

的商业软件，通常有专门的测试人员负责查找软件漏洞，当找到一处漏洞时，会直接向相应的代码编写维护人员请求修复。但是在开源软件的供应链体系中，一段有漏洞的代码很可能短时间内找不到相应的维护人员，即便开源项目主导者收到了通知，可能并是他自己具体负责的部分，不能及时修复。一个常用的开源软件模块被修复时，理想的情况是能够快速同步到其他所有使用了该模块的开源项目中去，而不是同一个漏洞被一次次的在不同软件中反复发现，反复修复，浪费人力物力，甚至被攻击者反复利用。开源代码维护人员的稳定和及时响应，以及大规模、全覆盖的修复推送，正是消除开源软件供应链漏洞传播风险的关键所在。

（4）持续维护风险

开源软件的长期义务维护可能会导致一系列不公平的现象，例如商业公司通过开源软件赚取了丰厚利润，但并没有给维护者任何回馈，甚至会刻意回避谈及对开源软件的使用，由此引起开源维护者的反感甚至一些过激行为。近期发生的faker. js与colors. js开源库遭作者恶意破坏的事件就是典型的例子。

随着开源模式的普及，开源软件供应链会越来越清晰呈现在产业界面前，不仅贯穿整个信息技术产业，同时也渗透到其他各行各业，成为生产生活的基础要素。而开源软件供应链存在的问题也将无法回避，需要全球开发者、开源社区甚

至政府机构共同解决。

三、 开源软件供应链重大基础设施

（1）意义：保障产业的开源软件可靠供应

尽管我国已经开始积极推动开源生态的建设，但国内开源软件产业仍面临着根本问题。首先是产业价值不高，以美国红帽（Red Hat）公司和国内主要操作系统厂商对比为例，前者在 2019 年的收入约为 30 亿美元，而后者同时期年收入则在亿元人民币规模。其次，创新创业支撑不足。近年来，美国诞生了一些基于开源的独角兽企业，如著名的开源协作软件 Slack 和开源云计算软件 Snowflake，市值分别达到 200 亿和 700 亿美元。在国内，极度缺乏这样基于开源的高价值的创新创业公司。其三，开源生态受限。华为在 2019 年报发布会上指出，谷歌依托安卓操作系统的 GMS（谷歌移动服务）对华为断供，至少影响了 100 亿美元的海外销售收入。

事实上，开源软件供应链“持续供应”问题频频发生，已经给国内软件产业敲响了警钟。例如，Docker 是云计算领域最重要的开源应用容器引擎。2020 年 8 月 13 日起，它的企业版 DockerEE 和 DockerHub 禁止被美国政府列入贸易管制“实体清单”的企业使用，一批中国企业、科研院所和高校受到直接影响。CentOS 是国内服务器领域使用最多的开源操作系统，2020 年 12 月，红帽公司宣布将于 2021 年年底停止

维护 CentOS 8，给中国企业造成了大量的应对成本。再如 Openwall 组织的“隐形断供”问题，漏洞共享、安全预警是操作系统等基础软件产业的重要支撑环节，然而由于获取 Openwall 的漏洞共享信息受限，国内基础软件存在 2 周以上的“安全预警空白区”。

除此之外，国内的开源软件供应链还面临新型 OpenChain 的“准入”风险。OpenChain 是开源软件合规性标准，目标是在交换开源软件解决方案的组织之间建立信任基准，确保程序被设计成为合规工件。当前 OpenChain 已成为 ISO 5230 国际标准，意味着国内开源软件企业未来可能必须符合 OpenChain 标准才能进入国际市场。但国内本就缺乏开源软件的合规性审核，这一标准的实施将限制国内软件产品进入“国际大循环”。

当前俄乌局势中，欧美众多商业软件对俄罗斯“断供”，引发全球关注。相比之下，开源软件和开源社区具备更为中立的属性，即便发生禁用，也具有更大的应对弹性。

（2）开源软件供应链重大基础设施的建设

中国科学院软件研究所在 2019 年启动了开源软件重大基础设施建设，旨在支撑开源产业的高质量可持续发展，提升开源产品的开发效率与产品质量，打破商业软件的价值链和供应链垄断。

重大基础设施的核心环节之一便是建设开源软件图谱，软

件图谱通过刻画软件基本属性、软件之间依赖关系，以及软件的可维护性等信息，从而支撑包括知识产权风险、软件质量风险、安全风险和可维护性风险在内的多维度风险评估。

通过开源软件的精细化全生命周期管理，实现对国内 10 余类关键基础软件行业供应链的风险管控。目前，基础设施平台囊括了开源软件数量超过 630 万个，代码量超过 100 亿行,软件图谱实体数量超过 1300 万个,节点属性超过 781 种，关系数量超过 1.8 亿条，收集许可证超过 2400 个，细粒度许可证协议分析超过 2400 个。在此基础上，研究和构建了国内规模最大的漏洞图谱，数据维度多样，包含 12 种实体，26 种关系，136 种属性；数据量丰富，涵盖了 1346727 个实体，超过 2053 万条关系。漏洞图谱进一步刻画了软件安全相关概念及关系，包含漏洞、缺陷、攻击、威胁情报等信息，从而支撑对供应链的安全性进行评估。

截至目前，基础设施平台已为 openEuler 开源社区、OpenHarmony 开源社区、RISC-V 生态等提供了重要支撑。接下来，开源软件供应链重大基础设施建设将努力实现一系列重要目标。例如为软件科学研究提供所需的高质量开源代码大数据，并提供高度结构化的数据组织形式，从而支撑软件工程的智能化，为代码合成、机器智能编程等信息技术前沿领域奠定基础；为关键设备和系统提供高质量、低风险的开源软件供应链，降低开发成本，提升开发效率，打破商业软

件的垄断。

此外，中科院软件所还将面向开源软件人才培养与人才汇聚，持续开展“开源软件供应链点亮计划”（OSPP，Open Source Promotion Plan），发动全社会力量，消除开源软件供应的已有和潜在风险。

四、 总结

开源软件已成为信息社会的“原材料”和“元器件”，开源软件供应链基础设施意义重大。中科院软件所已经进行了大规模开源软件知识图谱构建，并深入推进软件源代码的安全、知识产权和维护性风险评估研究。开源软件供应链重大基础设施建设将是“软件新基建”的一次重要实践，也是与国内龙头企业、高校院所、开源社区、联盟协会等共同为国产软件产业“定魂筑根”、在国际开源领域融入与贡献的一次重要实践，任重道远，未来可期。

参考文献：

[1] 梁冠宇,武延军,吴敬征,赵琛.面向操作系统可靠性保障的开源软件供应链.软件学报,2020,31(10):3056-3073.

开源知识产权

简析开源相关的法律风险

梁帆

一、开源协议简述

开源软件许可证从法律的观点来看相当于一份一份的合同约定，只不过这种许可合同并非协商得到，而是事先规定好的标准化合同。目前对于开源社区常用的许可证有：

GPL——使用了任何 GPL 代码的软件，都必须将完整的源代码公开，并允许他人修改、发布。对于适用 GPL 许可协议的软件，该软件的修订版或衍生作品也应通过适用 GPL 许可协议的相同条款进行分发或许可。

LGPL——相较于 GPL，对商业化更友好，在 LGPL 下发布库时，链接到该库的软件不需要开源，基于该库修改而得到的软件仍然需要遵循 GPL 许可证进行开源。

MPL——如果被许可人没有修改原始软件并使用原始许可协议，则被许可人对 MPL 许可的软件拥有新的著作权，被许可人可以使用其他许可协议对软件进行再许可

Apache——许可给使用者著作权以及专利权。

BSD——仅要求被许可方在分发软件时识别原始著作权所有者，并注明免责声明，类似于 MIT 许可证，只要满足许可证设定的条件，就可以自由地修改并发布代码。

MIT——几乎最宽松，其对于开源代码的使用没有限制，只需保留著作权声明和许可证内容即可。

有时一个开源软件中会出现多许可证的问题，一般是由于不同分支最终导致的结果，因此要注意许可证的兼容问题。在决定将软件开源的许可证时，建议根据项目的特点和需求，从现有的许可证中进行选择。

各许可证的特点的已经总结的较为成熟，此处不再展开。

二、开源软件著作权风险

1.开源的本质和 copyleft

开源软件以创新的方式重新解释了专有软件行业赖以存在的基本法律基础。与使用著作权来“排他”的专有软件不同，开源提倡“包容”。开源的本质上是对软件进行著作权保护，然后对其进行大规模许可以供使用、改进或修改，开源是以互惠也被称为著佐权（copyleft）的方式回馈给软件社区，而著作权（copyright）则相反。这种开发模式会使软件随着后续用户的增加而在多方面呈指数级增长。这就是开源的创新性，其中放弃了一些传统的著作权利益，而带来了其他优势。

2.开源中的渗透问题

开源领域的一个主要问题就是开源代码渗透到其他代码中、或者其他代码渗透到开源代码中。根据不同的开源许

可，则有可能不得不向整个社区公开原本不想公开的代码。例如，某些代码根据 GPL 等许可证合并到某些软件的源代码中，可能会“感染”该软件，从而导致该软件根据许可证的条款自动获得许可，也因此必须遵守该许可。例如，微软便遇到过该渗透问题，在微软将具有 GPL 许可的部分代码合并到其 Hyper-V 驱动程序中后，才发现该部分代码感染了微软的 Hyper-V 驱动程序，而微软不得不向 Linux 贡献了该 Hyper-V 驱动程序的代码以避免违反 GPL。

三、开源中的专利权风险

1. 专利在软件中的问题

开源社区对软件专利是持有怀疑态度的，针对程序方面，例如专利期限的延长、放宽构建块程序（流程块）的非显而易见性的标准、不透明的起诉过程、不披露源代码、滥用延续申请等均是社区持有疑问之处。部分观点认为软件专利是创新的对立面，因为大量的块程序受到了保护，也就意味着一个软件的流程得到了保护，而软件的流程是相对简单便能想到的，最困难的部分是如何用代码实现、代码如何编写等；同时流程得到保护后，代码上的创新受到了遏制，因为即便有无数种创新方式去实现这一流程，也不会有开发者再去考虑了，毕竟一旦实现了也有可能会被专利权人控告侵权；并且块程序的专利本身与代码的基础逻辑就是相悖的。

目前在我国申请软件相关专利一般包含几以下种情况：(1)硬件控制软件，例如控制机械设备的运动的软件；(2)提高计算机内部性能的软件，例如可以提高计算机虚拟内存的软件；(3)外部数据处理软件，例如数码相机图像处理软件。大部分的申请可能属于第三种情况。

2.专利对开源的影响

软件专利对开源传播的模型构成的威胁不可小觑。如果某开源软件对某专利的侵权得到证实，即使是一小部分，基本上都会使得该开源软件停止开发。同时，开源软件的本质使它们容易受到专利方面的监控，这加深了开源软件的困境。

3.专利是否能够达到 copyleft

开源社区已尝试过通过许可条款，将开源软件的 Copyleft 的影响从著作权扩展到专利，即开放专利运动。例如，当分享软件时，软件开发者还可授予用户实施其持有的专利的许可。作品可以按原样使用或改进，当然在这种情况下，专利的改进方面必须重新授权给持有原始专利权的机构。

虽然将 Copyleft 适用于专利法的核心概念相对简单，但实际困难是多方面的。首先，著作权法和专利法对改进的处理存在根本区别。这主要是因为著作权权利人拥有控制软件改进的法定权利，即衍生作品受著作权保护，而专利则并非如此；其次，著作权保护从创作完成时即生效，但专利保护需要申请。如果对所做的每一项改进都去申请专利将非常

麻烦，并可能会因此造成开源项目的延迟甚至停滞；第三，与著作权不同，获得专利是一个繁琐且成本较高的过程，因此，很多开发者不愿意向社区免费发布专利。

尽管 copyleft 在激励行业走向专利共享方面确实取得了一定的成功，但相比于著作权，专利方面的 copyleft 可能更难以实现。

4. 行使专利权的复杂性

专利相对与著作权来说更加复杂，相较于著作权，在获取专利权和维持专利权上要投入更多，专利在申请阶段就需要提交和申请很多文件，而一旦出现潜在的侵权问题，专利的诉讼成本也高于一般的著作权诉讼的成本。因此发起专利侵权诉讼本身就是对专利权人来说需要极为慎重考虑的事情。

在另一方面，完全存在适用于许可软件但许可人和被许可人都不知道的专利。由于专利数量较多，开发者不可能了解世界上所有的软件。由于许可人只能许可属于他们的作品，因此特定软件许可的存在并不能保护被许可人免受第三方专利权人提出的侵权索赔。对专利风险的分析往往需要聘请律师来进行，成本也较高。

5. 开源圈对专利侵权诉讼的态度

2019 年 10 月，Linux 开源组织 Gnome Foundation 宣布他们被 NPE（不实施但许可专利以获利的组织）Rothschild

Patent Imaging 起诉专利侵权。在这场诉讼中，被告得到了广泛的支持，甚至知名律所的免费法律服务。该诉讼在 2020 年 5 月迅速和解，被告甚至得到了原告所有专利（而不限于起诉的专利）的免费许可。该案显示出开源社区对专利侵权诉讼的警惕和联合起来的巨大能量。

四、开源中的商业秘密问题

针对商业机密的诉讼案件，原告往往必须证明（1）其拥有商业秘密，以及(2)被告不当使用商业秘密。对法院来说，软件的不当使用是一个很容易就能判断的问题，根据协议的条款，可以直接地看到哪些行为是不当使用。但何为商业秘密是很重要的，而在开源这一领域，商业秘密的判断则比较困难，因为开源软件本身就开放了很多信息，哪部分能够构成商业秘密是未来需要探讨的方向。原告仅仅声称某些信息是商业秘密是不足以构成商业秘密的，更何况还会有一些例如将所谓的商业秘密披露给了第三方且第三方无需保密的情况。

五、认定受开源许可证影响的软件边界

1. 高传染性

在上述提到的案件一和三中，北京高级人民法院认为受 GPL 协议约束的软件中的插件并不受到 GPL 约束，而广州知产法院认同了 GPL 协议的“高传染性”，即在 GPL3.0 协议

下开源软件的衍生作品或修改作品也需要遵循GPL许可协议开放其源代码。

2.独立程序

在2019年，最高院审理的一件计算机软件作品著作权纠纷案中认为前端和后端代码是独立的不同代码，前端代码用于页面设计等，而后端代码用于实现软件本身的底层逻辑，因此认为前端代码与后端代码在实际达到的效果和最终结果存在明显不同，且法院认为不能仅仅因为代码的交互配合就认定二者为同一代码。最高院认为GPL的高传染性包括基于开源软件的衍生程序或修订版本，但不包括存在交互或联系的其他独立程序。正如计算机系统中的多数软件或代码需要互相配合以达到目的，但这些软件或代码并非同一软件或代码。

六、开源的界限

开源软件经常涉及技术的跨国界传播，因此也需要面对各国国家的技术管制相关法律。Open source 不等于 open border。

因为俄乌战事，全球最大的开源及私有软件项目托管平台Github官方发文称，其会遵守美国政府的相关规定，限制俄罗斯通过Github获得军事技术能力。而除了GitHub，越来越多的开源社区例如Node、js、知名前端框架React等都

在其官网上加入了声援乌克兰的标语。随后，SUSE、红帽、Docker 也纷纷宣布停止与俄罗斯的业务。

上述公司，例如 Docker，其作为一家美国公司，必须遵守美国在出口管制方面的法律法规。而为了遵守这些法规，在停止俄罗斯业务之前，Docker 已对一些国家进行了限制。2019 年，GitHub 出于美国贸易管制法律要求，也对一些国家的开发者用户进行了限制，甚至是封禁账号。其实由此可以看到，这些开源社区也是在不同国家的法律下建立起来的，其也必须遵守所在地的法律法规，因此，开源平台和开源企业实际上是难以保持中立的。

开源软件的开发与维护往往涉及到不同的主体，也就涉及到不同的权利归属、许可、授权等法律问题。例如 Linux 基金会自身的管理办法不受美国出口管制，但 Apache 基金会的管理办法明确说明遵循美国出口管制。

七、中国开源相关案例

近些年来随着开源软件在我国的发展，相关案例也渐渐出现在大家视野中，对于处于发展阶段的我国来说，目前案例并不多，相关法律也并不健全。当然对于这个较新的领域来说，国外也在发展和探索中。从近些年的案例来看，我国法院对于开源软件的态度越来越清晰，下面介绍几个比较具有代表性的案例：

1. 认可 GPL 在我国具有法律效力

2019 年，在审理一桩涉及 GPL 的软件著作权侵权案件中，北京高级人民法院在判决书中认可 GPL 为合法协议。

在该案中，原告开发了一款包含三个插件的软件，其主张被告开发的软件使用了原告的三个插件的源代码，侵害了其对该软件享有的著作权，并请求法院判决被告承担损害赔偿等法律责任。被告辩称原告的软件使用了 GPL 项下的程序，因此该三个插件程序也应适用 GPL，而开源软件协议允许使用 GPL 项下程序，因此其不构成著作权侵权。

法院最终判决不予支持被告提出的三个插件受 GPL 协议约束的主张。理由是被告认可涉案三个插件中并不包含 GPL 开源协议，在原告的涉案软件的根目录下也不存在 GPL 开源协议。

该案作为较早涉及到 GPL 的开源软件相关的著作权侵权纠纷案件，虽然没有深入探讨开源软件协议（如没有探讨 GPL 的内容等），但认可了 GPL 在国内具有法律效力。

2. 首例开源软件作为知识产权犯罪案件的无罪案

2021 年，南京某科技有限公司及高管涉嫌侵犯商业秘密一案在检察院作出三份《不起诉决定书》后以所有被告无罪结案。本案是国内首例获得司法机关判定的、以开源软件作为知识产权犯罪案件辩护事由的无罪案（也包括知识产权侵权之民事抗辩在内）。

在该案中，被告在 2003 年独立完成与涉案软件同种类的系统软件并享有软件著作权，而该系统软件中包含有 GPL2.0 开源协议的声明。涉案软件其为根据前述系统软件改进而来的软件，部分程序的代码来自于该 2003 年开发的系统软件。

该案中的检察机关认可GPL的法律效力,并同时认可GPL协议的强传染性。最终认定被告于 2003 年开发的系统软件是基于GPL 协议的开源软件,并且基于该软件开发的新软件、撰写的新代码均属于GPL 开源软件。最后检察院认定“具有非公知性的证据尚不充分，本案不符合起诉条件”。

3. 对于开源软件协议若干核心法律问题更深的探讨

2021 年 9 月，广州知识产权法院对一宗涉及开源软件的侵权案做出一审判决。广州知识产权法院在本案的判决书中深入地阐述了法院对 GPL3.0 开源许可协议的性质及条款的理解。

该案于 2019 年 3 月立案，争议焦点为以下几方面：1) 开源软件的著作权归属；2) 开源许可协议的性质及开源软件侵权行为的认定；3) 对开源软件侵权行为的法律救济。

针对开源软件的著作权归属问题，被告主张涉案软件为项目管理者和相关贡献者共同创作的、不可分割使用的合作作品，由各方共同享有著作权；而原告则主张只有创作双方具有合作创作的合意和合作创作的行为才构成合作作品。

法院认为：（1）原告公司的股东作为项目管理人于2016年将涉案软件的初始版本源代码进行开源发布，为1.0版本开源软件代码的核心基础，而其他贡献者仅在此基础上进行代码的升级优化，且由项目管理人决定是否采用该些代码，因此其他贡献者提交的代码并未对涉案软件著作权产生实质影响；（2）根据我国《著作权法》，合作作品的认定需要满足四个要素：作者为两个或两个以上、主观上有共同创作的合意、客观上有共同创作的行为以及合作作者贡献了独创性的表达。但根据本案证据，无法认定本案涉案软件属于合作作品；（3）涉案软件使用LGPL3.0或GPL3.0开源协议，其他贡献者在申请将其代码合并入主分支时即默认同意使用相关开源协议，也就意味着同意将其修改增补的代码贡献给项目管理者和其他用户，授权其在许可协议范围内自由使用；（4）原告提交了著作权登记证书，被告虽否认其著作权人身份，但并未提供证据。因此法院认定本案原告拥有涉案软件的著作权。

针对开源许可协议的性质及开源软件侵权行为的认定，法院探讨了三方面：1. GPL3.0的性质及违反GPL3.0的法律后果；2. 是否可以在GPL3.0中附加商业使用限制；3. 违反GPL3.0行为及开源软件侵权行为认定。

针对GPL3.0的性质以及违反其法律后果，法院认为：违反相关开源许可协议规定的使用行为构成侵权行为；在中国

法下，GPL3.0 协议的内容具备合同特征，条款明确规定了使用相关开源代码的方式，授权内容也符合中国著作权法的规定，合法有效；GPL3.0 协议属于附解除条件的著作权合同，许可条款是著作权许可的条件，而如果使用者违反条款规定，则许可的前提条件已不复存在，其所获得的许可授权也自将自动终止，相关使用行为也将构成侵权行为。

针对 GPL3.0 中附加商业使用限制，法院首先认为只要某个软件版本加入了 GPL3.0 协议，就无法删除该协议，相关开源版本的源代码将永久保持开源。权利人只能在后续其他更新的版本中变更或删除 GPL3.0 协议，但不影响此前的开源版继续适用 GPL3.0 协议。法院认为权利人无权在 GPL3.0 协议中加入商业使用限制保留条款：开源软件不等于不能有商业开发，GPL3.0 协议序言就强调所谓自由软件（free software），并非价格免费；GPL3.0 第 7 条规定了六种可以添加的补充附加条款，其中不包括商业使用限制保留条款；而不属于第 7 条规定的条款都被视为第 10 条规定的不可以对 GPL3.0 协议所授权的权利进行“进一步限制”的条款。

法院认为被告构成侵权的行为是未向用户提供被控侵权软件的源代码。按照 GPL3.0 协议的规定，在发布包含适用该协议的源代码的程序副本时，无论收费还是免费都应该确保副本的接收者也能够得到源代码。

针对法律救济，法院认为在理论上存在违约救济和侵权

救济两种方式，在违约救济下，守约方可以获得的救济主要是继续履行合同和损害赔偿；在侵权救济下，被侵权人可以获得的救济包括停止侵害、损害赔偿、恢复原状和临时禁令救济等；违约救济下的损害赔偿责任范围小于侵权救济下的损害赔偿责任范围。救济方式由当事人自行选择。

相较于前述案件中法院并没有对 GPL 的传染性问题进行探讨,广州知识产权法院则在本案的判决中认可了 GPL3.0 的合法性并认同其“高传染性”,即认可在 GPL3.0 协议下,开源软件的衍生作品或修改作品也需要遵循 GPL 许可协议，开放其源代码。虽然广州知产法院对前述问题进行了深入探讨，但依然有很多问题值得进一步研究。

人工智能（脑机接口）

脑机接口动态

本刊编者[5]

全球和国内研发脑机接口（BCI）技术已启动，迄今COPU已收到国内外脑机接口人工智能跟帖留言35条（其中来自美国的13条，来自国内的10条）。

脑机接口技术指在人脑中植入芯片连接神经元，并与脑外机器连接起来，由人的意志（思维或想像力）利用人脑神经元（EEG、脑电图）来操控机器。

脑机接口可用来治疗中风、癫痫患者或治疗老年痴呆症、自闭症等疾病，也有这样的实例：用意念打字，或用人眼超高精度摄像，也有用于截肢患者，让其用意念来控制取代残肢的机械手，进行三维活动（如顺利进食、进水、取物和握手等动作）。

2019年8月8日，COPU接受美国卡内基梅隆大学研发团队发来第一例脑机接口跟帖。

近年来，脑机接口发展无创连接技术，无需开颅向大脑植入芯片。

2016年，我国发射天工二号实验室，天津脑科学中心、天津大学对航天员实行无创脑机接口技术，《nature》

[5] 本刊编者：陈伟、鞠东颖。

杂志主刊为此发表“自然聚焦——中国脑科学”栏目系列：“脑机接口——梦想之光照进现实生活”。

今年4月30日，东南大学、华南理工大学、北京大学信息科技学院、新加坡国立大学、广州琶洲实验室、英国格拉斯哥大学联合组成脑机接口研发团队，通过非侵入性脑机超平台，成功实现人脑直接无线通信。

美国开展首次脑机接口人体临床试验

本刊篇者[6]

据报道，马斯克脑机接口公司 Neuralink 的竞争者 Synchron 公司近期宣布开始在美国进行名为“COMMAND”研究的首次人体临床试验，首位 COMMAND 患者在纽约西奈山医院参加了临床试验。

Synchron 开发了一种名为 Stentrode 的设备，以帮助严重瘫痪的病人。该公司的目标是让患者能够通过血管内的脑部植入物控制数字设备，而不是用手控制。Stentrode 穿过颈静脉，到达大脑。它是由一种网状材料制成的，有 16 个传感器，可以扩展到血管壁上。Synchron 公司的 Stentrode 连接到胸部的一个电子设备上，该设备转发来自运动皮层的大脑信号。

[6] 本刊编者：陈伟、鞠东颖。

敬请关注联盟微信公众号
COPU开源联盟

扫描二维码
获取往期资料

中国开源软件推进联盟秘书处　　电话：+86 010-88558999
联盟公共邮箱：office@copu.org.cn　　联盟官网：http://www.copu.org.cn
地址：北京市海淀区紫竹院路66号赛迪大厦18层