从俄乌冲突看我国开源安全发展

近年来，开源在各行业各领域得到广泛应用，国内的开源生态整体呈现蓬勃发展的态势。据统计，我国企业软件几乎都会使用到开源代码，流行开源软件被近 1/4 的软件项目使用。然而，由开源软件的依赖关系，自然形成的供应链包含从编码、打包、分发各个环节，其中任何一环出现问题，都可能导致开源软件面临重大风险。开源安全已成为当前亟需重视的问题。

一、俄乌冲突中涉及的开源领域事件

近期随着俄乌冲突的爆发，美国为首的西方国家联合全球盟友对俄罗斯展开了全面围剿，并在政治、经济、文化、体育和科技等领域推出一轮又一轮的制裁措施。尤其是在科技领域，为了限制俄罗斯在高科技领域的竞争力及获取美国先进技术的能力，美国总统拜登 2 月 24 日发表讲话，强调美国及其盟友将对俄罗斯展开“毁灭性的制裁行动”。美国商务部通过工业和安全局（BIS）正式公布了针对俄罗斯的一系列全面的严格出口管制措施，包括半导体、芯片、计算机、电信设备、加密安全设备、激光和传感器等。美国商务部长 Gina M. Raimondo 明确表示：“商务部与我们的国际合作伙伴以及本届（拜登-哈里斯）政府将继续使用我们所拥有的一切工具手段来限制支持俄罗斯军事能力的产品、软

件和技术。”

随后，以美国公司为首的科技巨头相继宣布制裁俄罗斯。硬件方面，英特尔、AMD、联想、戴尔、台积电、思科、三星、苹果等科技企业宣布停止对俄罗斯供货；软件方面，微软、SAP、Oracle、亚马逊等软件巨头宣布停止在俄罗斯的产品销售和服务。这意味使用这些巨头产品的企业、机构业务将面临瘫痪。

与此同时，开源界也牵扯进俄乌之间冲突的漩涡中。世界最大的代码托管平台和开源社区 GitHub 表示，严格限制俄罗斯获取维持其侵略性军事能力所需要的技术；前端三大主流框架之一 React 声援乌克兰，英文官网首页上线支持乌克兰的横幅；影响力巨大的编程语言 PHP 社区邮件讨论列表出现了一封“申请援助乌克兰”的邮件，目的在于呼吁 PHP 社区火速参与俄乌冲突；最大的开源包管理系统 Node.js 公开表态站队乌克兰，并在官网首页新增了一段带话题的呼吁性文字，表示与乌克兰人民站在一起；全球第二大开源代码托管平台 GitLab 已暂停在俄罗斯和白俄罗斯的新业务；全球市场排名第二的开源 Web 服务器 Nginx（由一名俄罗斯工程师 Igor Sysoev 开发并开源）的母公司 F5，取消了俄罗斯对 F5 的网络访问，并停止了在俄罗斯对 Nginx 开源项目的贡献；开源项目 vue-cli（vue-cli 是一个基于 Vue.js 进行基础架构快速开发的完整系统，称为脚手架工具。）的依赖

项 node-ipc 包正在以反战为名进行供应链投毒，如果主机的 IP 地址来自俄罗斯或白俄罗斯，该代码将对其文件进行攻击，将文件全部替换成❤。

根据俄罗斯研究小组维护的一个开源“抗议软件”清单（链接在文末），目前已经有多达 30 个开源项目加入了对俄罗斯的抵制，其中甚至包括亚马逊（AWS Terraform modules）和 Oracle 等科技巨头的项目，也不乏 MongoDB、pnpm、es5-ext、Drupal、RedisDesktopManager 等流行项目。上述开源项目的抗议方式多种多样，包括数据和代码库销毁、加载恶意软件勒索软件、DDoS 攻击、植入后门等高危行为到屏蔽俄罗斯开发者或者显示政治标语等中低烈度的抗议行为。这些行为对俄罗斯的经济运行和 IT 行业造成了严重冲击，以至于俄罗斯总统普京于 2022 年 3 月 30 日签署总统令：为保障技术独立性，要求从 3 月 31 日起禁止在国家采购中未经相关部门许可为重要国家基础设施部门购买外国软件，从 2025 年开始，国家重要基础设施部门将完全禁止使用外国软件。

开源政治化的潘多拉盒子已经打开，虽然开源社区一向推崇“自由、平等、相互尊重”的原则，开源精神被无数开发者奉为圭臬，然而“封锁”事件的上演，令国内开源开发者们开始担心，“开源无国界”是否为伪命题？一旦此类事件发生在我国，我国的开源软件如何保证自身的安全？

二、我国开源软件安全现状

现代软件已经从单体模式演进到以开源软件为代表的规模化协作模式。复杂软件往往涉及诸多开源软件，这些开源软件彼此组合、依赖，连同为各个开源软件做贡献的维护者和开发者，共同形成庞大的供应关系网络。据统计,不管是手机,还是电脑,平均每个程序都要依赖150个开源组件。开源事实上成为了软件开发的核心基础设施，混源软件开发也已成为主要软件开发交付方式，开源的安全问题也已被上升到基础设施安全和国家安全的高度来对待。尤其是随着乌俄冲突下的科技制裁，对我国的开源领域安全再次敲响了警钟，我国开源领域面临的安全风险主要有技术安全、供应链安全、开源政策法律及应用安全。

（一）开源技术安全

1.开源软件漏洞数量保持高位

根据新思（Synopsys）公司《2021开源安全和风险分析报告》，Black Duck审计服务团队在2020年审计的涵盖17个行业的1546个流行代码库中,98%的代码库包含开源代码,75%的代码由开源代码构成，84%的包含至少一个漏洞，每个代码库平均有158个漏洞，65%的代码库存在许可证冲突。

根据GitHub官方数据显示，2018年新增开源漏洞数也创下近6年新高，新增 7563 个漏洞， 2019年与 2020 年

增长率略有下降，2020 年发布的漏洞数较 2019 年发布漏洞数少了 1746 条。具体数据见下图：

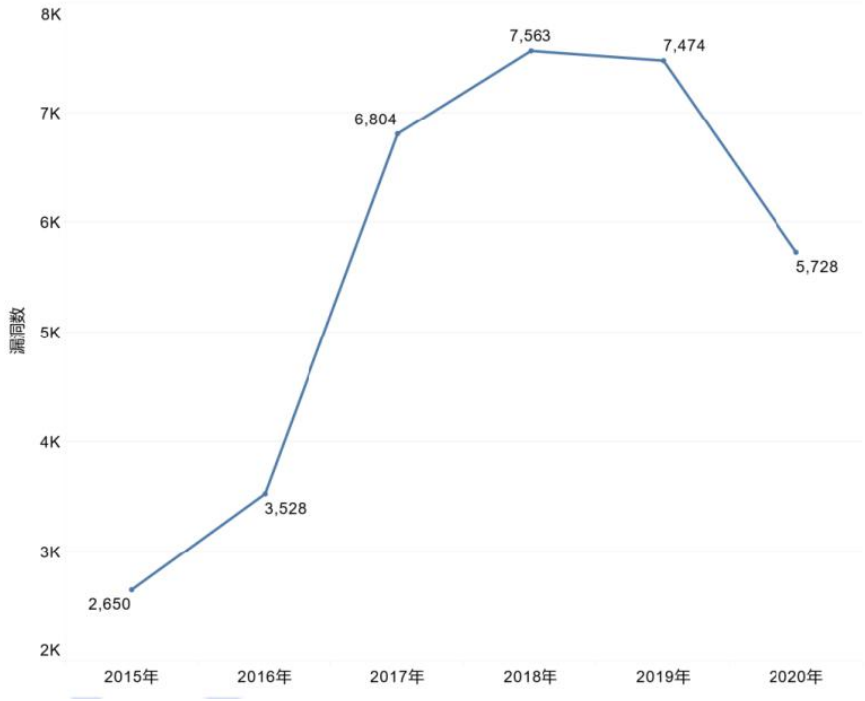

图 1:开源漏洞时间分布

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 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。输入验证、路径遍历、跨站脚本、注入、NULL引用、资源管理、密码管理、API误用、配置管理、日志伪造等十类安全缺陷是程序员在编写软件代码时经常会出现的典型安全缺陷。在2020年检测的1364个开源软件项目中，十类典型安全缺陷的总体检出率为56.3%，每类典型缺陷的检出率及排名如下表所示。

表1：主要漏洞类型

排名	缺陷类型	检出率
1	输入验证	34.9%
2	路径遍历	30.7%
3	注入	28.6%
4	NULL引用	24.8%
5	API误用	24.3%
6	资源管理	20.7%
7	跨站脚本	19.1%
8	日志伪造	17.9%
9	密码管理	13.8%
10	配置管理	12.9%

据 CNCERT 的《2021 年开源软件供应链安全风险研究报告》调查显示，缺陷类型 CWE 79 越界写入的数量最多，占 2020 年新增开源漏洞的 14%左右。下表列出了 TOP 10 CWE 缺陷类型，这些缺陷类型很容易并被利用，往往通过系统信息暴露、窃取数据或阻止应用程序正常工作等方式，对系统造成安全风险。

表 2：2020 年开源漏洞 TOP 10 CWE 缺陷类型

CWE 编号	中文名称	个数
CWE-79	在 Web 页面生成时对输入的转义处理不恰当（跨站脚本）	824
CWE-506	内嵌的恶意代码	726
CWE-400	未加控制的资源消耗（资源穷尽）	510
CWE-200	信息暴露	305
CWE-20	输入验证不恰当	212
CWE-94	对生成代码的控制不恰当（代码注入）	201
CWE-119	内存缓冲区边界内操作的限制不恰当	142
CWE-125	跨界内存读	134
CWE-78	OS 命令中使用的特殊元素转义处理不恰当（OS 命令注入）	124
CWE-325	缺少必要的密码学步骤	117

2.开源软件漏洞影响范围巨大

根据新思（Synopsys）公司《2021 开源安全和风险分析报告》，2020 年再次发现了 2019 年前十大开源漏洞（包括一个高风险漏洞），其中一些漏洞的百分比显著增加。CVE-2019-10744 在这两年的代码库审计中出现率均为 29%，该漏洞对常用 JavaScript 库 4.17.12 之前的所有版本均有影响。

以 2021 年影响最大的 Apache Log4j2 漏洞事件为例。2021 年 12 月，Apache Log4j2 被发现其某些功能存在递归解析功能，存在攻击者可直接构造恶意请求，触发远程代码执行的漏洞。根据工信部发布的《关于阿帕奇 Log4j2 组件重大安全漏洞的网络安全风险提示》，该漏洞可能导致设备远程受控，进而引发敏感信息窃取、设备服务中断等严重危害，属于高危漏洞。

据 Check Point Research 统计漏洞爆发 4 天(自 12 月 10 日至 12 月 13 日）情况报告，在 Apache Log4j 2 漏洞发现早期的 12 月 10 日，黑客尝试利用该漏洞进行攻击的次数仅有几千次，但这一数据在隔天却增至 4 万次。而漏洞爆发 72 小时后，捕捉到利用该漏洞尝试攻击的行为就已超过 83 万次：

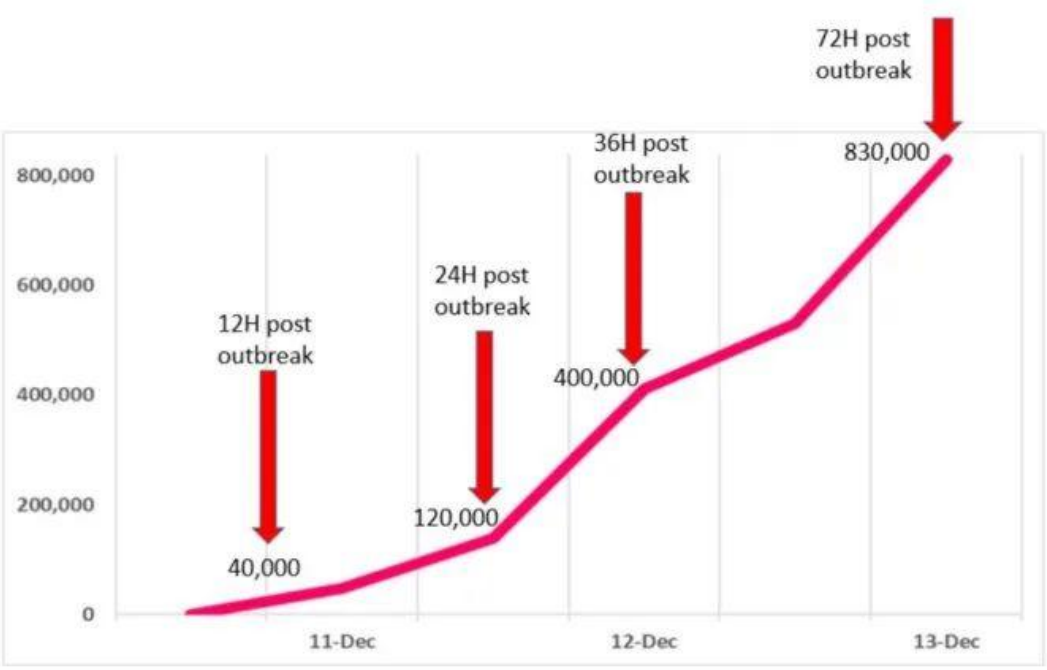

图 2：基于 Log4j 2 漏洞的攻击数量迅速上升

不仅攻击次数在持续攀升，基于该漏洞的新变种也在短时间内迅速衍生。Log4j 2 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。并且由于 Apache Log4j 2 应用范围大、漏洞修复较为复杂，而利用漏洞却十分简便，因此这个 Apache Log4j 2 漏洞很可能在未来几年内也将一直存在。

（二）开源供应链安全

1.大企业垄断开源生态阻碍创新

开源一直秉承鼓励创新的发展理念，已成为推动全球数字科技创新的重要因素。数据表明，开源技术支撑了 90%以上的互联网产品，推动了一大批小而精的创新型企业发展壮

大。开源倡导开放、共享的模式，兴起之时就遭到众多科技巨头的坚决抵制，但随着开源势不可挡地发展，全球科技巨头转而持续加码开源领域，纷纷通过收购开源平台强化其垄断地位，试图通过掌控开源平台不断强化对科技生态的领导力，并使得社区从早期的高度分散的技术架构转变为由几个强大的网络巨头所控制的架构。这种“大公司拥抱开源”的现象，一方面因大公司拥有在更高级别上开发和维护开源项目所需的资金，推动产生了更多的开源重点项目，并有助于提高质量和安全性；另一方面，受商业利益等因素驱使，通过对开源社区项目的开发和商业化推广，对开发人员施加种种限制，易造成技术垄断，并最终阻碍技术创新。

在过去十年中，从 Linux 和 MySQL 到 Kubernetes、Spark、Presto 和 MongoDB，开源一直是云创新的支柱，但部分大型云服务商正在改变开源的形态，可能会破坏开源创新的激励因素。大型云服务商很容易获取到优质的开源项目，并将其作为托管服务提供个客户。这些大企业并没有动力去回馈开源社区，很自然地从这些别人的工作中获得不公平的利润，从而破坏了开源创新所需要的发展动力。如果这种现象持续存在，将会极大地对开源从业者创办企业和获得投资方面产生抑制作用。

另外一些国际巨头不断通过垄断开源生态，在产业链中具有掌握极大话语权，并以此获益。例如谷歌旗下的操作系

统安卓、浏览器 Chrome、深度学习框架 TensorFlow、容器编排引擎 Kubernetes 等，分别在各自的领域占据优势地位，这些开源产品自身具有一定通用性和适用性，便于后续开发者 “不重复制造轮子”而在其产品的基础上进行进一步开发，但又通过人为制造诸如广告服务、有意破坏其他竞品连接谷歌服务的用户体验等方式排除竞争者获得垄断地位，最后从高达 30%谷歌应用商店抽成，内置安卓系统的 Google ADs，以及 GMS 服务授权费用等途径获得高额的垄断利润。尽管这些产品本身都是开源的，但是中小企业和个体开发者在面对谷歌限定的服务接口、苛刻的商业条款等问题时，很少有能力再进行创新并反馈开源社区，开放共享的初心被完全破坏殆尽。

2.小型开源项目维护压力增大带来不确定性

当一个开源代码库变得越来越受欢迎时，其代价就是其维护人员承受的压力就会越来越大，随之产生一系列运维相关问题。大量的项目处于失去维护的风险中，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%。统计的八个典型的开源软件包生态系统 Maven、NPM、Packagist、Pypi、Godoc、Nuget、Rubygems、Swift 中 NPM 的不活跃项目数量最多，达到 1018533 个，Rubygems 的不活跃项目比例最高，占比达到

86.5%，具体数据见下表。

表 3：开源软件包生态不活跃项目数量

序号	包生态系统	项目总数	不活跃项目数	不活跃项目比例
1	Maven	487799	272555	55.9%
2	NPM	1559835	1018533	65.3%
3	Packagist	309125	208890	67.6%
4	Pypi	287113	170044	59.2%
5	Godoc	234579	143685	61.3%
6	Nuget	307336	187238	61.0%
7	Rubygems	163392	141259	86.5%
8	Swift	77015	59521	77.3%

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，许多软件项目中使用了十几年前发布的开源软件版本，存在很大的运维风险。被使用的老旧开源软件版本中，最老旧的一个是 2003 年 3 月 3 日发布的 Apache Xalan 2.5.D1，已经有 18 年之久，但仍然被 7 个软件项目所使用。版本的更新滞后还导致多年前的漏洞仍留于多个软件项目中。最古老的漏洞是 2005 年 11 月公开的 CVE-2005-3510，仍然存在于 31 个项目中。

而在 Black Duck 团队 2020 年调查报告中中，有 91%使用了在过去两年中没有发生任何开发活动的开源依赖项，

85%的代码库含有至少四年未曾更新的开源依赖项。代码库使用的开源库并非最新版本，甚至经常是很旧的版本，根源就在于开发团队难以支撑开源项目维护的巨大投入。

2020 年初，JavaScript 的模块化标准库 core-js 的作者 Denis Pushkarev 因交通肇事被判处 18 个月监禁。Denis Pushkarev 是 core-js 项目唯一的维护人员，该项目周下载量 达 2600 万次，在 npmjs.com 上被 19279 个包依赖，重要程度可以认为是前端的基础设施。后续，GitHub 社区通过将账户所有权转移暂时缓解这一问题。

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。由于 faker.js、colors.js 代码库的历史版本仍存在于相关平台上，用户可及时降级为旧版本解决。后续，项目仓库 GitHub 还暂停了该作者对自己所有公共和私有项目的访问，

该事件发生后也有其他开源项目作者发出相似的声明。

1 月 11 日，另一个开源项目 Apache PLC4X 的创建者 Christofer Dutz 也在开源托管平台 GitHub 中发文，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。

（三）开源政策法律及应用安全

1.开源许可证法律效力有待进一步明确

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，比 2019 年略有减少。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。

对于包含没有明确定义许可证的开源代码依赖项的代码库，需要决定是否完全替换掉这些依赖项。按行业划分，

存在开源许可证冲突的代码库比例最高的行业 (86%)是能源和清洁科技以及制造业、工业和机器人行业。零售和电子商务行业中存在开源代码许可证冲突的代码库的比例最低，为 47%。

国内司法实践中逐步开始重视开源许可证的法律效应。2021 年 4 月，广东省深圳市中级人民法院审理罗盒公司诉风灵公司案的一审判决，该案明确指出 GPLv3 协议是一种民事法律行为，具有合同性质，可以认定为授权人和用户间订立的著作权协议，属于《合同法》调整的范围。此案例是国内首个明确 GPLv3 协议法律效力的案例，对开源许可证的法律界定，对开源软件侵权行为的判罚作出了有益的探索。

2.开源技术低门槛易获取等特点诱使技术滥用

技术的滥用既指打着技术的名号招摇撞骗，也指忽视风险的盲目技术创新。随着开源社区逐步成为技术创新的重要平台，在开放共享理念下不断降低一系列新兴技术的门槛，但这也给投机者和浑水摸鱼者可趁之机。例如，随着一些 AI 技术的开源，换脸制作不仅价格大幅下降，门槛也不断降低，“AI 换脸”“deepfake”等视频换脸技术门槛降低，普通人也能制作换脸视频，这项技术被用于恶搞视频、色情视频合成上，其不良效应也引发了社会的关注和担忧。

另一方面，攻击性安全工具（OST）是否可以不受限制的发布已成为信息安全领域最具争议的话题之一。OST 是指在不利用软件自身缺陷或漏洞的情况下，以合法身份实施入侵或规避安全防御机制的软件代码库。根据具体问题和应用场景的不同，OST 的功能往往也各不相同。OST 通常由信息安全专业人士开发，目的是促进网络安全相关技术的发展。然而不幸的是，这些 OST 代码往往因具有攻击能力，OST 将直接被黑客用来开发新的恶意软件，进行非法的网络攻击或数据窃取，技术滥用已经成为网络安全领域不可忽视的方面。

更为严重的是，一些国家为了发现软件代码漏洞为目的，开源使用了多年的网络战争软件，为黑客开展恶意网络攻击提供了便利，为网络空间安全稳定和网民合法权益带来巨大威胁。开源社区应坚持技术向善，让技术真正服务于实体业务，推动技术创新积极正向发展。

三、我国开源软件安全面临的不足

开源带来的正面效应已在数字经济生活中发挥重要作用，如何在安全可控的情况下使用开源，已成为我国高质量发展数字经济的关键任务。然而，目前我国开源生态仍处在发展阶段，开源软件供应链渗透度与参与度不足，对开源软件风险抵抗能力较弱。尤其在俄乌冲突中，不断有开源厂商

或组织因政治立场或个人情感的因素宣布断供封锁俄罗斯，粉碎了“开源无国界”的假象，这让开源倡导的“创新、开放、自由、共享、协调”理念，在所谓“政治正确”面前不堪一击。为了应对开源软件尤其是开源软件供应链存在的安全问题，有必要作出深入的分析，找出我们的不足，并提出相应对策。

1.开源软件面临的供应链“卡脖子”风险

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，美国纷纷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，市值分别已经达到了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，开源生态受制于人。谷歌依托安卓操作系统的GMS（谷歌移动服务）对华为断供，至少影响了华为100亿美元的海外销售收入。

事实上，开源软件供应链“卡脖子”事件频频发生，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 的“隐形断供”。Openwall 是开源基础软件安全预警平台。漏洞共享、安全预警是操作系统等基础软件产业的重要环节，可国内在这个领域仍然处于空白状态。由于获取受限，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。Linux 基金会采用快速过会的方式将 OpenChain 转变成国际标准，意味着国内软件企业必须符合 OpenChain 标准才能进入国际市场。但国内本就缺乏开源软件使用的合规性审核，这一标准的实施平添了壁垒，将限制国内软件产品进入国际“大循环”。

尤其在俄乌冲突中，虽然有悖于开源精神，但是仍有多个开源组织还是表明了政治立场，把政治带入到开源项目中，抛弃了技术中立立场。如著名的开源项目 Nginx，作为一个俄罗斯工程师发起并开源的项目，由于被美国公司 F5 收购，在俄乌冲突中，F5 停止了在俄罗斯对 Nginx 开源项目

的贡献，并表示 Nginx 将在俄罗斯没有任何代码，无论是商业还是开源代码；GitHub 和 GitLab 这两个在世界上排名第一、第二的开源代码托管平台直接管理海量的开源项目，对开源项目有着巨大权力，以至于在俄乌冲突中，两大平台都对俄罗斯采取了“封号”“限流”等措施，成为国际政治角力的重要手段之一。究其原因，在国际开源软件生态中，大量主流的开源软件多由美国的基金会和社区主导，而美国出口管制法律法规（包括 ECRA、EAR）对“根据美国法律设立的任何组织形式的实体”都有约束力，无论是否明确说明，美国相关企业都要遵循美国出口管制法律法规。这表明如果未来中美冲突加剧，将会给我国的开源软件供应链带来一定的风险。

我国目前也在构建由我国主导的开源基金会与开源联盟组织，加强开源生态的建设。然而相较于国外，我国的开源生态起步较晚，在整个开源软件供应链中渗透和参与度低，导致对国外开源生态依赖较强，在开源软件供应链层面缺乏自主与主导能力。

2.开源用户面临的风险层出不穷

在俄乌冲突中，开源项目 vue-cli 的依赖项 node-ipc 包以反战为名进行供应链投毒，该包在 npm 每周有上百万下载量，依赖的下游开源项目面临巨大安全风险。随着越来越多的开源项目成为软件基础设施的核心组成部分，开源项目自身的开发安全也愈发重要。近年来，开源软件断供、投毒、恶意删库、利用开源软件漏洞的网络攻击等事件层出不穷，

这次 node-ipc 库中被植入恶意代码就是一个典型的案例。

除 node-ipc 事件外，近期还发生多起开源软件供应链安全事件，比如 Apache Log4j2 漏洞事件、faker.js、colors.js 删库事件、Linux“脏管道”事件、周下载量超过 700 万次的 JavaScript 流行库 ua-parser 账户遭接管事件、影响多家大厂的依赖混淆事件、SolarWinds 事件、PHP 源代码事件等等。当前，从开源软件供应链安全的角度来看，国内监管机构已准备陆续推出相关标准及政策，但针对关键基础设施和重要信息系统相关的企业和单位，并没有制定具体的举措和细则要求。

3.开源软件供应链风险大但研究投入少。

俄乌冲突涉及开源领域的事件带给我们的警示，一定要重视开源软件供应链安全风险的研究和预防，否则将为我国的开源生态、数字技术与科技产业发展埋下严重隐患。根据中国科学院软件研究所相关研究表明，开源软件供应链主要面临三大风险，即安全性风险、可维护性风险以及合规风险。为应对上述风险，国外包括谷歌、微软、IBM、亚马逊、Linux 基金会、Apache 基金会等商业机构和基金会共同开展相关研究，并启动了诸如 OpenSSF、Sigstore、OpenChain 等相关项目，对开源软件供应链风险进行持续研究，并提供防控手段。

- OpenSSF：由 Linux 基金会的牵头成立的开源软件安全基金会，旨在将广泛的社区领导者聚集到一起，建立具有针对性的计划和最佳实践，以提升开源软件的安全性。OpenSSF 收到的金融资助来自多家科技巨头如亚马逊、思科、戴尔、Facebook、谷歌、Intel、微软和 Oracle。这些资助将帮助 OpenSSF 找到并解决开源软件中的安全漏洞，从而确保软件供应链的安全。该基金会还着手开发最佳实践、工具、培训和漏洞披露实践。
- Sigstore：旨在全面覆盖开源代码社区，允许开发者轻松地为软件提供签名。结合出处、完整性和可发现性，此举有助于营造透明且可审核的软件供应链。
- OpenChain：作为 Linux 基金会下的项目，旨在制定开源软件供应链标准，帮助各种组织更高效地解决开源许可证一致性地问题。通过 OpenChain 认证后，开源许可流程将更为轻松。目前 ARM、微软、谷歌、高通等各领域巨头纷纷加入 OpenChain，为开源软件供应链的标准制定做出贡献。

相比之下，我国在开源软件供应链安全方面的研究基础比较薄弱，亟需从国家、行业、机构、企业各个层面建立开源软件供应链安全风险的发现能力、分析能力、处置能力、防护能力，整体提升软件供应链安全管理的水平。

四、北京发展开源软件供应链安全的建议

从俄乌冲突中可以看出，只有在核心领域掌握核心技术，才能在关键时刻不被卡脖子。在国家“十四五”规划中提及，补齐产业链、供应链短板，实施产业基础再造工程，加大重要产品和关键核心技术攻关力度，发展先进适用技术，推动产业链供应链多元化。因此，为了贯彻落实发展开源软件的国家战略，实现开源软件的可靠供应，增强我国信息化设施的自主可控，亟需提升我国的开源软件供应链安全管理水平。北京作为我国软件与信息技术服务业收入最高、规模最大、从业人员最多、科研实力最强、开源软件生态最齐全的城市，非常有必要建设一个可靠的开源软件供应链，夯实数字经济发展基础。

1.加强开源软件供应链风险发现与防控技术研究

建议发挥北京软件的产业、人才与学术资源优势，联合在京的基础软件公司、互联网公司、开源软件公司、网络安全公司以及高校和科研院所、国家信息安全漏洞库平台等核心单位，开展开源软件供应链风险发现与防控技术研究，为在京政府、企业、机构等提供安全、可靠、可持续的开源软件供应链保障。鼓励和支持有条件的企事业单位、社会组织开展开源软件供应链图谱梳理工作，从开源终端产品到原始开发者，绘制详细开源供应链图谱，筛选脆弱环节，强化供

应链安全风险预警。

2.构建开源供应链风险评估体系和预警机制

建议联合相关单位，从开源软件供应链安全性风险、可维护性风险以及合规风险角度出发，制定开源软件供应链风险评估标准，并建立包含评估工具、测评与认证在内的开源软件供应链风险评估体系，鼓励企业对其商业化软件产品进行开源软件供应链风险评估，以提升软件产品安全可靠性。制定开源供应链安全行为准则，实时监测国内开源软件供应链的重点事件。从战略政策层面，持续关注跟进开源国际形势，实时跟踪了解国际开源软件供应链的动态，特别是各国在开源软件供应链方面的政策举措及落地方案。

3.建设并北京开源软件供应链安全基础设施。

建议在北京联合有关科研院所、企业、社会组织、开源社区等机构共同建立一个基于开源软件安全的创新联合体，汇集北京开源资源，建设北京开源软件供应链安全公共基础设施，为在京的各类涉及开源的机构、企业、高校及研究院所提供包含开源软件供应链漏洞感知、开源软件关键节点识别、威胁监测、风险预警、风险评估等多种基础安全服务，建立全球开源供应链预警机制，实现对供应链各环节中开源软件来源的溯源机制，实现对全球开源应用及其安全缺陷的预测预警。降低各行业对开源软件供应链风险发现和处置成

本并提升相关风险的应对能力，通过公共基础设施平台加速开源生态能力建设。

4.进一步引导和推动相关行业参与并贡献开源。

鼓励和引导各行业在应用开源的同时，增加对开源的参与和贡献程度，尤其对于开源软件供应链中的关键节点，积极探索和掌握开源技术核心，并促进相关开源技术的迭代升级。对于掌握核心技术的开源社区与开源项目，可协助对接京内具有相关开源技术需求的企业，适当给与政策与资金支持，加速开源生态建设与开源技术成熟。