大洋理事会谈开源政策翻译与学习笔记

开源软件的安全在现在这个时代是十分重要的，涉及开源软件 (OSS) 的高调安全事件已引起美国、欧盟及其他地区政策制定者对 OSS 的普遍性及其社区所面临独特挑战的关注。对于希望支持 OSS 作为共享资源的安全性和可持续性的政策制定者来说，这整篇报告基于一个重要视角：OSS作为基础设施。OSS 是在允许任何人检查、修改和重新分发源代码的许可下发布的代码。这有助于开发者共享和重复使用解决方案，从而提高效率，有些人估计 97% 的软件依赖于 OSS。OSS 范围广泛，从用于图形显示的小组件到完整的操作系统。贡献者包括在业余时间工作的个人、大型公司的员工、基金会及其他人。OSS 生态系统是基于社区的，拥有多种治理结构来管理贡献和维护。

本报告将 OSS 与三种基础设施系统——水资源管理系统、资本市场以及公路和桥梁网络——进行了比较，并借鉴了每个系统现有的政策机制，以提出支持 OSS 作为共享资源的可持续性和安全性的政策建议。

软件借用了水系统的比喻，包括软件包与依赖它们的最终产品之间的“上游”和“下游”关系。使用地下水或河水的实体不会假设水质永久适用，而是会确保水符合其不同需求。同样，OSS 的使用者有责任确保他们使用的 OSS 得到良好支持和保障，而 OSS 的最大用户对生态系统的可持续性负有最大的责任。OSS 还与资本市场相似，面临着复合的系统性风险，因为软件依赖链可能使一个 OSS 项目成为多个下游系统的单点故障。这些风险在消费者或监管者缺乏透明性或准确报告来评估和缓解风险的情况下加剧。最后，OSS 以前被比作道路和桥梁，这种比喻体现在持续支持不足随着时间的推移会带来风险。桥梁倒塌——或广泛使用的 OSS 软件包中的漏洞被发现——会引起关注和投资，但为了防止这些危机而进行的持续、常规维护往往被忽视。

综上所述，这些基础设施系统及其支持的政策机制为希望将 OSS 作为基础设施支持的政策制定者提供了关键原则。

**鼓励负责任的OSS消费：**

1. 让政府“身体力行”成为负责任的OSS消费者，通过在联邦政府内部设立一个或多个开源项目办公室，帮助各机构管理其OSS战略、政策和关系。
2. 通过美国国家标准与技术研究院（NIST）开发一个包含风险评估和对OSS生态系统反馈贡献的OSS最佳实践框架。行业和政府可以使用该框架进行自我评估，政府也可以利用该框架来帮助进行采购评估。
3. 通过成熟的OSS公司和非营利组织制定一套标准的最佳实践，以鼓励更多小型组织的“OSS好撒玛利亚人”参与OSS贡献。

**减轻系统性风险：**

1. 在网络安全与基础设施安全局（CISA）内设立数字系统性风险管理办公室（ODSRM），负责识别系统性数字风险，包括关键的广泛使用且面临风险的OSS软件包，以便进行有针对性的支持。

**提供以安全和可持续性为中心的资源：**

1. 建立一个机会导向的资助计划，以支持系统性重要的OSS项目的维护和事件响应工作。
2. 设立OSS信托基金，以提供对OSS代码的安全性和维护的可持续、长期投资，并支持OSS维护者社区的健康发展和规模扩大。
3. 开发一个“领养软件包”项目，通过该项目，公司可以提供资源来支持其依赖的OSS软件包的持续维护和漏洞缓解。这类项目可以鼓励更多的小型公司和非IT行业公司参与。

开源软件 是由全球社区开发的，没有专属所有权，它使得工程师、科学家和企业家能够共同创造巨大的技术进步。

OSS 及其代码和开发者对世界的影响长期以来在专家社区之外没有得到足够的重视。

Nadia Eghbal 在2016年的开创性研究帮助揭示了OSS在构建关键技术系统时面临的公共政策挑战。OSS不仅仅是一个安全性不足的问题，其开发模式还提出了一个关于公平和价值的基本问题。OSS 将**销售价值**（消费者愿意为免费产品支付的价格）与**使用价值**（消费者通过使用该产品获得的收益）分离出来，这一问题早在1997年就由Eric Raymond指出。

该报告基于大西洋理事会及其他机构的先前研究，以及开源政策网络（Open-Source Policy Network）收集的见解，旨在论证公共政策可以通过将开源软件（OSS）视为基础设施来解决其系统短板。通过将OSS作为基础设施制定支持和维持的政策，有助于消除对安全漏洞的恐惧，转而将OSS视为高效软件生态系统的关键组成部分，同时仍然承认政策在改善整体安全性方面的重要作用。

虽然开源作为一种理念早于互联网——如1969年Unix诞生时的混乱许可和开发价值体系就是一个例子——但互联网极大加速了OSS的发展。

开放源码软件项目与更大的软件世界之间的关系也很复杂，而且千差万别。 这里有一个 有用的术语叫 "堆栈深度"，指的是开放源码软件和其他组件在整个产品或应用中的埋藏 深度。开放源码软件最直接的用途可能是面向用户的应用程序

可以将开放源代码视为许多不同的、相互影响的生态系统。它们不断发展、对刺激做出反应、竞争、合作、拥有文化并遵循规范。影响开放源代码生态系统的行为可能会产生超出该生态系统的连锁反应，甚至超出专有技术甚至整个技术的世界。

开放源码生态系统及其众多利益相关者早已认识到项目需要持续、稳定的支持，并通过建立非营利组织和机构来提供支持。政府根据社区需求和政府优先事项（如安全或创新）提供支持，可以为开放源码软件世界中现有的零散组织和项目提供强大、稳定的支持。根据三个类比归纳出三个类别：政府支持与资助、生态系统风险实践以及开放源码软件消费者的负责任使用。CSIS 数据集还描述了这三类政策之外的其他政策--有的在政府内部设立了专门管理各种开放源码软件功能的办公室，通常被称为开放源码计划办公室（OSPOs）；有的要求将政府开发的数据和解决方案开源；还有的描述了采购实践。

开放源码软件实际上与专有软件没有太大区别：所有代码都可以更安全地开发，而且开放源码软件面临的安全风险在大多数数字系统中都很常见。对于开放源码软件来说，不同之处在于开放源码消费者--从政府到私营部门再到最终用户--与他们所依赖的项目之间的关系。由于缺乏明确的交易关系，以及贡献者社区的多样性和不断变化的深远影响，政策和行业在充分引导和支持方面面临着挑战。其结果是，这个生态系统既促进了数字创新，又常常因开发人员负担过重、社区和项目资源不足而受到影响。

我们使用的大部分代码都不是我们自己编写的。在认识到这一点并在无限期的未来接受这一点的同时，开放源码软件以及开发和维护它的众多社区应该在任何网络安全和经济健康分析中占据重要地位。开放源码是我们信任敏感数据、关键社会项目以及经济发展和创新周期的基础设施。这些基础设施正因需求的重压而日渐衰弱 ，在某些地方甚至摇摇欲坠 ，这不应比桥梁倒塌的景象和地下水中毒的报道更令我们震惊，因为这些都是由于维护不足和广泛使用造成的。

开放源码软件是一种基础设施，因此，为其提供支持将使其在经济和政府活动的关键领域得到更迅速的采用和大量的创新。

大多数人常常认为日常事务和问题的妥善解决是理所当然的。然而，无知和未能保护它们的代价是高昂的。Log4shell、一系列开源软件包事件 以及开放源码软件维护者对从劳动中获取价值而不做出回报的经济模式的担忧，都是选择继续无知的表现。风险在于一个充满活力的生态系统的缓慢崩溃，以及未来在少数技术公司集中之外，数字开发的多样性和能力的下降，从而危及国家安全和经济竞争力。好在这种崩溃既不是必然的，也不是永久的。变革是可能的，也是亟需的，但变革必须以投资和政策的形式出现。一个健康、有弹性的开放源码生态系统可以带来一美元几分钱的价值，这种投资提供了一种手段，可以确保重要的数字基础设施免受各种威胁。对开放源码软件的大力投资和知情政策首先是给当代人的一份礼物，而不仅仅是对后代人的抽象捐赠，它将影响和保护全世界的社区。