Atlantic Council
CYBER STATECRAFT INITIATIVE

Avoiding the Success Trap: Toward Policy for Open-Source Software as Infrastructure

Executive Summary

This report offers a framing for policymakers seeking to support the security and sustainability of open-source software (OSS) as a shared resource: **OSS as infrastructure**. It uses policy vehicles from more familiar forms of infrastructure to inform recommendations that promote the responsible use of OSS, address systemic risk, and provide resources to the OSS ecosystem with sustainability in mind.

Water Management

Like the largest entities in water ecosystems—dams, treatment plants, distributors, and more—OSS consumers must ensure that what they draw on meets their requirements of use. As in water conservation, the largest OSS consumers carry the most responsibility to contribute back to the ecosystem's sustainability.

Capital Markets

Both capital markets and OSS act as enabling inputs for many other industries. Capital markets also highlight the creation of risk from complex interdependencies and the need for transparency to manage it—dynamics both present in the OSS world.

Roads and Bridges

As in critical transportation infrastructure, routine, mundane maintenance is more useful in the long term than responding to sudden collapse or crisis, yet it is often overlooked.

for more information or to get involved, check out the full report at https://www.atlanticcouncil.org/in-depth-research-reports/report/open-source-software-as-infrastructure/

Final Thoughts

OSS is central to modern digital systems. Relationships with the OSS community are necessarily, and substantively, different from those that government and industry have grown accustomed to. Encouraging sustainable OSS usage practices reflects the responsibility of the largest consumers for managing much of the risk associated with software use, including OSS, and better addresses OSS-specific features of development and contribution. Addressing systemic risk is an important step for policy efforts to support the security and sustainability of OSS projects with an accurate picture of the considerable interdependencies among code bases. Governments can step up and provide substantial resources to support OSS as the infrastructure it is.

Authors:
Stewart Scott
Sara Ann Brackett
Trey Herr
Maia Hamin

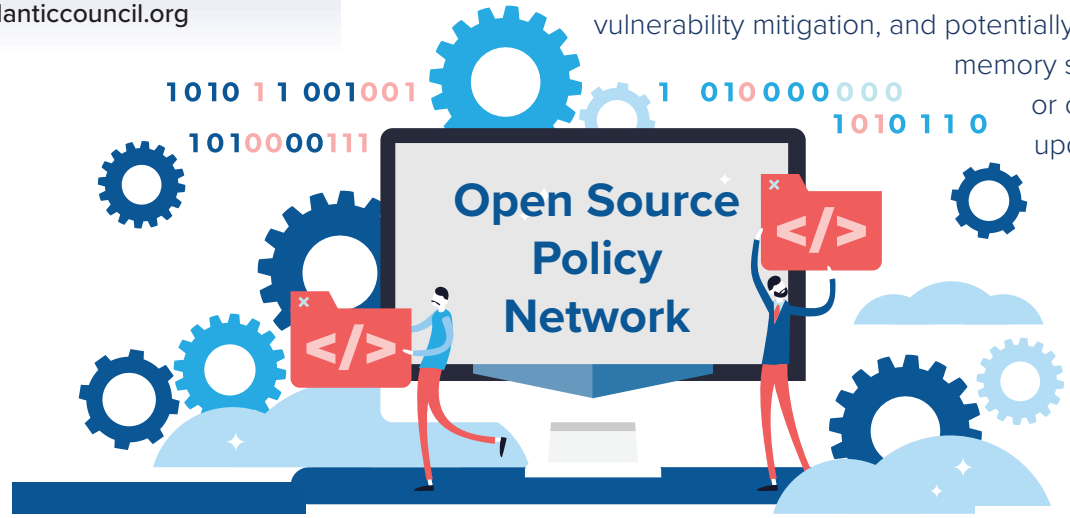
For any inquiries please reach out to therr@atlanticcouncil.org

Policy Recommendations

- **Encouraging Sustainable OSS Participation**
  1. **Start By Improving Government Consumption:** create institutional entities with an explicit mandate to focus on the federal government's use of and support for OSS, modelled after OSPOs recently established by other organizations.
  2. **Support Private-Sector Consumption:** develop an OSS Usage Best Practices framework through NIST with significant industry input.
  3. **Protect OSS Good Samaritans:** draft best-practices standards for contributing to and supporting OSS projects.

- **Address systemic risk**
  4. **Establish an Office of Digital Systemic Risk Management (ODSRM):** create a government office responsible for, in close cooperation with industry, identifying and channeling support to critical OSS projects used widely throughout industry and government systems, as well as studying patterns of dependency.

- **Provide Resources with Security and Sustainability in Mind**
  5. **Target of Opportunity:** create funding programs to support OSS security. The goal of this funding is to award resources in a targeted manner, determined by government need, to OSS projects and activities.
  6. **Establish the OSS Trust:** create a broader mechanism for governments to provide consistent support for the security of OSS code, the integrity of OSS projects, and the health and size of OSS maintainer communities.
  7. **Adopt-a-Package:** define programs by which firms and other donors can "adopt" important, unmaintained packages and provide resources to support their ongoing maintenance, vulnerability mitigation, and potentially rewrites into memory safe languages or other structural updates.



with generous support from Craig Newmark Philanthropies, Schmidt Futures, Omidyar Network, OpenSSF Open Source Security Foundation