ÉTUDES DE L'IFRI

GEOPOLITICS OF TECHNOLOGY PROGRAM

DECEMBER 2022

Software Power

The Economic and Geopolitical Implications of Open Source Software

Alice PANNIER

The French Institute of International Relations (Ifri) is a research center and a forum for debate on major international political and economic issues. Headed by Thierry de Montbrial since its founding in 1979, Ifri is a non-governmental, non-profit organization.

As an independent think tank, Ifri sets its own research agenda, publishing its findings regularly for a global audience. Taking an interdisciplinary approach, Ifri brings together political and economic decision-makers, researchers and internationally renowned experts to animate its debate and research activities.

ISBN: 979-10-373-0641-8

How to quote this publication:
Alice Pannier, "Software Power: The Economic and Geopolitical Implications of Open Source Software", *Études de l'Ifri*, Ifri, December 2022.

Ifri

27 rue de la Procession 75740 Paris Cedex 15 – FRANCE

Tel. : +33 (0)1 40 61 60 00 – Fax : +33 (0)1 40 61 60 60

Email: accueil@ifri.org

Website: Ifri.org

Author

Alice Pannier heads Ifri's Geopolitics of Technology program, launched in October 2020, after having been associate researcher since 2019. Her research focuses on European technology policy and Europe's external relations. Her recent publications include: "Digital Sovereignty: Review of Macron's Term and Debates in the 2022 Presidential Campaign" (*Briefings de l'Ifri*, March 15, 2022) and "Strategic Calculation: High-Performance Computing and Quantum Computing in Europe's Quest for Technological Power" (*Études de l'Ifri*, October 6, 2021).

Prior to joining Ifri, she was Assistant Professor in International Relations and European Studies at the Paul H. Nitze School of Advanced International Studies (SAIS) at Johns Hopkins University, Washington D.C. (2017-2020). A graduate of King's College London and Université Paris 1 Panthéon-Sorbonne, she holds a PhD from Sciences Po Paris.

Aknowledgment

The author wishes to thank Rubén Pépin for research assistance and for the translation of the study into English.

Executive Summary

Open source plays a central role in software development, both in parallel with proprietary software and increasingly intertwined with it. It has become a major factor for companies' innovation processes and for the success and popularity of their products. For users, using open source software can alleviate risks stemming from proprietary solutions, including data privacy concerns or trade restrictions. Beyond that, open source is the foundation of critical software bricks and Internet languages and protocols.

However, open source is a victim of its own success. It suffers of a lack of resources dedicated to the maintenance of open source components, even though vulnerabilities in open source code can have serious consequences, as illustrated by the Log4Shell vulnerability in December 2021.

For these reasons, private companies are investing ever more money and human resources in the development and maintenance of open source software, and acquiring structuring roles in the governance of the ecosystem. This support, however, is not without risk for the open source ecosystem, which is increasingly shaped by the private interests of Big Tech companies.

Meanwhile, governments are getting increasingly concerned with the cybersecurity implications of open source software, and with risks not only of accidental vulnerabilities, but also manipulation of codes by criminals and foreign agents. The interest of governments in open source is not new, but it is evolving: governments are no longer only seeking to adopt open source or to develop software solutions, but also to contribute to the financing or even the governance of open source ecosystems, at the national and/or global level.

An analysis of the United States, Chinese and European cases show that government involvement in open source is not only pragmatic; it is increasingly politicized, and serves to uphold governments' ambitions for national security, international influence, or digital sovereignty. The study highlights the dilemmas that emerge, for public authorities, from the tensions between the desire to secure universally used, critical open source components, the desire to develop "sovereign" technologies, and the risk of encroaching on the horizontal and decentralized functioning of open source.

Résumé

L'*open source* tient une place centrale dans le développement des logiciels, sur un mode à la fois parallèle au modèle propriétaire, et de plus en plus imbriqué avec celui-ci. Il est devenu un élément déterminant dans les processus d'innovation des entreprises du numérique et pour le succès et la popularité de leurs produits à l'échelle mondiale. Plus encore, l'*open source* est au fondement de briques logicielles critiques et des langages et protocoles d'internet, et joue un rôle dans le développement de technologies émergentes.

L'*open source* peut toutefois être victime de son succès et souffre d'un manque de moyens dédiés à sa maintenance. Or, les vulnérabilités dans les codes sources ouverts peuvent avoir de graves conséquences, comme l'a illustré la faille « Log4Shell » révélée en décembre 2021.

Les entreprises privées investissent financièrement et humainement au développement et au maintien de l'écosystème. Ce soutien est critique pour pallier les risques liés au manque de maintenance de certains composants. Cependant, cette implication n'est pas sans danger pour l'écosystème *open source*, qui est de plus en plus modelé par les intérêts privés des *Big Tech*.

Parallèlement, les gouvernements sont de plus en plus préoccupés par les risques de l'*open source* en matière de cybersécurité, non seulement du fait de vulnérabilités accidentelles, mais aussi de la manipulation des codes par des criminels et des agents étrangers. L'intérêt des gouvernements pour l'*open source* n'est pas nouveau, mais il évolue : les gouvernements ne cherchent plus seulement à adopter l'*open source* ou à développer des solutions logicielles, mais aussi à contribuer au financement ou même à la gouvernance des écosystèmes *open source*, au niveau national et/ou mondial.

L'analyse des cas américain, chinois et européen montre que l'implication des gouvernements dans l'*open source* n'est pas seulement pragmatique ; elle est de plus en plus politisée et sert à soutenir les ambitions des gouvernements en matière de sécurité nationale, d'influence internationale ou de souveraineté numérique. L'étude met en évidence les dilemmes qui émergent, pour les autorités publiques, des tensions entre le désir de sécuriser des composants *open source* critiques universels, le désir de développer des technologies « souveraines », et le risque d'empiéter sur le fonctionnement horizontal et décentralisé de l'*open source*.

Table of Contents

Introduction

One of today's technological trends is the ever-increasing "softwarization" of human activities, i.e. the use of software for a growing number of activities at the individual, corporate and government levels. The transformation of industry, the digitization of public services, the deployment of 5G, and the advent of the Internet of Things are all factors that contribute to the increasing strategic importance of software. As a result, as the Linux Foundation explains in a recent report:

> "Vulnerabilities and weaknesses in widely deployed software present systemic threats to the security and stability of modern society as government services, infrastructure providers, nonprofits and the vast majority of private businesses rely on software in order to function."[1]

Aside of being everywhere, this software is getting more and more complex, in its functionalities and components, creating new risks, and triggering a necessary evolution of security analyses.[2]

At the heart of software is open source code.[3] It is estimated that 80% to 96% of the code that makes up software on the market today – including proprietary software – is of open source origin.[4] Some are critical technology building blocks for widely used software and web servers around the world. Whether they know it or not, most companies, individuals, and governments use open source software or components. According to David Nalley of the Apache Software Foundation, "Open source is not just an important part of the software industry, it is one of the foundations of the modern global economy".[5] In addition, all emerging technologies, such as Artificial

1. Linux Foundation and OpenSSF, "The Open Source Software Security Mobilization Plan", White Paper, 2022, p. 3.
2. ANSSI and CEA, "L'ANSSI et le CEA renforcent leur collaboration en cybersécurité", Press communication, June 29, 2022, available at: www.ssi.gouv.fr.
3. It is necessary to justify the choice of the term "open source" and to distinguish it from the term "free software". Free software is based on four freedoms defined in the late 1980s by Richard Stallman of the Free Software Foundation: freedom to run the program, freedom to study how it operates, freedom to redistribute copies (for free or not), freedom to make improvements, and freedom to share them. Software developed through open source generally meets the requirements for "free" software, and vice versa; in fact, one often refers to "free and open-source software". However, open source refers to a way of developing software rather than to a type of license, since open source components are found in most proprietary software. In this study, we prefer to use the term "open source", which refers indiscriminately to software or its components.
4. Synopsis, "2022 Open Source Security and Risk Analysis Report", April 2022; K. Szulik, "Open Source Is Everywhere: Survey Results", Tidelift, April 12, 2018, available at: https://blog.tidelift.com; T. Herr, "Responding to and Learning from the Log4Shell Vulnerability", testimony to the Committee on Homeland Security and Government Affairs, United States Senate, February 8, 2022.
5. D. Nalley, "Responding to and Learning from the Log4Shell Vulnerability", testimony to the Committee on Homeland Security and Government Affairs, United States Senate, February 8, 2022.

Intelligence (AI) and the Internet of Things (IoT), include elements developed in open source, so the strategic importance of the phenomenon will continue to grow.

This fact raises several questions. Why and how has OSS become such a structuring element of the global digital infrastructure and economy? How is the global open source ecosystem organized today? What links and tensions exist between open source and the dominant private actors? How are governments addressing this issue, and with what possible consequences for the ecosystem?

In the first part of the study, we will see that open source raises cybersecurity issues and also economic and innovation issues. Open source offers gains for software development, whether in terms of speed, quality, transparency of components and possible vulnerabilities, interoperability, or autonomy of use. Paradoxically, however, OSS suffers from well-known weaknesses that have to do with the mainly voluntary nature of the work of contributors and maintainers of open source projects, including the most critical ones.

For these reasons, open source is currently the object of increased attention, and specific strategies, from private and public actors, who seek to make the most of open source. In the second part, we will examine the role of the major players that structure the open source ecosystem. The large technology companies were the first to take up this challenge, both for practical and economic reasons. In fact, they already play a structuring role in the open source ecosystem, which is also organized around large foundations and code repositories.

Finally, we will analyze the role of governments, where awareness of the strategic stakes of open source at the highest political level is recent, but growing. An analysis of the United States (U.S.), Chinese and European cases show that government involvement in open source is not only pragmatic; it is increasingly politicized, and serves to uphold governments' ambitions for national security, international influence, or digital sovereignty. The study also shows that it is not easy to find a balance between the willingness to secure critical open source components with a global reach, the desire to develop "sovereign" technologies, and the risk of encroaching on the horizontal and decentralized functioning of open source.

The Rise of Open Source Software: Opportunities and Challenges

The development and distribution of software are structured around two major licensing models, and by extension, economic and political models: proprietary software and open source software. Proprietary software was initially dominant but has some limitations, such as high economic costs and risks, especially in light of international geopolitical competition. At the same time, open source has risen to prominence over the last twenty years, and open source software or software components have become central to the global digital infrastructure. However, it is becoming increasingly difficult to distinguish between the two models, due to the growing hybridization of software development processes. In addition, the ecosystem is confronted with cases of cybersecurity breaches, and a structural lack of resources allocated to the maintenance of certain components. All these elements that have attracted the attention of both companies and governments.

Open Source at the Heart of the Digital Infrastructure and Economy

The Quest for an Alternative to the Proprietary Model

From the dawn of the Internet era in the 1970s until the late 1990s, proprietary software proliferated and became dominant.[6] In the proprietary model, the software is usually developed by a private entity for profit. The software is paid for and made available to the customer through a licensing system or, especially for software available from the cloud, through a subscription. Other sources of revenue for software publishers include maintenance contracts, the sale of associated services and "premium" functions, and advertising.[7] In the proprietary model, the source code of the software is generally not accessible to the user, and therefore the software cannot be examined or modified.

6. K. Brigham, "How Open-Source Software Took Over the World", CNBC, December 14, 2019, available at: www.cnbc.com.
7. European Union, "The Economic and Social Impact of Software & Services on Competitiveness and Innovation", SMART 2015/0015, 2017, p. 25.

The dominance of proprietary software has since been challenged. For users, the proprietary software model poses a set of problems and risks, which partly explain the willingness of companies, governments and individuals to resort to alternatives, such as free and open source software. The context of global geopolitical competition increases the risks associated with dependence on proprietary software, especially when it is produced by foreign firms: cybersecurity risks and low visibility of these risks, dependence on extraterritorial legislation (especially concerning the processing of data resulting from software use), and even restrictions on trade and use of certain software for political or national security reasons.

Proprietary Software: Cyber… and Physical Risks

There are debates in the expert communities about the respective advantages of proprietary and open source software with regards to cybersecurity, but it is generally accepted that the impact of a security flaw in software depends above all on the extent of its use.[8] Consequently, the dominant software publishers have a particular responsibility in terms of the security of their products, and of informing users in the event of a security breach. These security guarantees especially important for security-critical software, such as those that perform functions that are critical in terms of user trust (privileges or direct access to networks and machines, for example).[9] Antivirus software, in this logic, is critical because of its intrusive nature.

The recent experience of the SolarWinds attack is an illustration of the severe impact that a flaw in critical software can have. The Orion software, developed by SolarWinds, is a system performance monitoring tool installed in thousands of organizations in the United States, including the U.S. government itself. Orion was targeted by a malware, revealed in December 2020, that allowed attackers to gain access to affected data, networks and systems for many months.[10]

Finally, in the context of the rise of connected objects and IoT, we can mention the case of embedded software. For example, accidents involving the Boeing 737 MAX aircraft in 2018 and 2019 were caused in part by errors in the aircraft's software, after its development was outsourced and unsupervised.[11] This type of cybersecurity issue is likely to increase with connected objects, especially in the automotive industry.[12]

8. Business Software Alliance, "Open Source and Commercial Software: An In-Depth Analysis of the Issues", 2005, pp. 8-12.
9. Federal Register, "Improving the Nation's Cybersecurity", Executive order 14028, May 12, 2021.
10. Sonatype, "État de la chaine logistique logicielle en 2021", 2021, p. 13.
11. P. Robison, "Boeing's 737 Max Software Outsourced to $9-an-Hour Engineers", *Bloomberg*, June 28, 2019.
12. R. Csernatoni and M. Blumenthal, "Computers on Wheels: Automated Vehicles and Cybersecurity Risks in Europe", Carnegie Europe, March 24, 2022.

Concerns over Data Protection and Platform's Policies

Other issues related to proprietary solutions concern data protection, and fears related to the exfiltration and non-consensual exploitation of this data. One of the risks is the possibility of backdoors deliberately built into proprietary software, which can affect any type of device.[13] Recently, attention has focused in Europe on made available in the cloud in a Software as a Service (or SaaS) mode. These may be subject to the laws of the country where the software providers are based, and therefore subject to obligations to transmit user data to the authorities of their country. The concerns related to American cloud service providers are well known, and regularly reiterated by the French and European authorities.[14] Concerns are even greater for Chinese suppliers. For example, while Alibaba is expected to host data for the Paris Olympic and Paralympic Games in 2024, the French general secretary for national security and defense warned "the possibility of 'exfiltration of databases [...] for strategic purposes or economic espionage' or 'pre-positioning' in networks 'to carry out subsequent actions'", if the Organizing Committee uses the services of the Chinese supplier.[15]

These kinds of concerns are not limited to cloud software. Mobile phone applications, such as social networking app TikTok is also coming under increased scrutiny from several governments due to concerns about how user data may be handled when transferred to China. Since 2020, the Indian government has even banned the use of TikTok, as well as other Chinese apps, for this reason.[16]

Another recent trend relates to concerns about the practices of large platforms, such as social networks, regarding their content management and moderation policies. Illustratively, in the fall of 2022, the debates around Twitter since its takeover by Elon Musk, have brought to the forefront the existence of open source social networks, such as Mastodon, as alternatives to the platform and its excesses.

Restrictions on Trade and Use of Software

Finally, a set of risks that are less widespread at this stage, but of concern to companies and governments alike, relates to (potential) restrictions on the trade and use of proprietary software, depending on its country of origin or destination. While these trade restrictions on software, some of which date

13. M.-G. Bertran, "La place des logiciels libres et open source dans les nouvelles politiques du numérique en Russie", *Hérodote*, No. 177-178, 2020, p. 245.
14. Commission de la Défense nationale et des forces armées de l'Assemblée nationale, "Audition, à huis clos, de M. Stéphane Bouillon, Secrétaire général de la défense et de la sécurité nationale", full report, July 13, 2022, p. 6.
15. A. Guiton, "JO 2024 : pour la protection des données, les autorités veulent déminer le problème Alibaba", *Libération*, July 26, 2022.
16. D. Milmo, "TikTok's Ties to China: Why Concerns Over Your Data Are Here to Stay", *The Guardian*, November 8, 2022.

back to the Cold War, mainly concern software for military use, they tend to extend to a growing set of software used in engineering and technology development, such as semiconductors.[17] Thus, some software, including American software qualified as "U.S. Origin" cannot be sold in China.[18] These restrictions may have indirect effects: if certain technologies have been developed using U.S. software that is subject to restrictions, these technologies are subject to U.S. controls, since under the Foreign Direct Product Rule (FDPR), a U.S. license is required to (re)export certain products developed using U.S. machines or software to China and other countries. In addition, under the technology transfer restrictions, a user of cloud solutions may unintentionally violate certain restrictions if the services used online are routed through foreign countries without the user's knowledge.[19]

While these controls generally concern cutting-edge technologies, restrictions may be placed on more widely used software. For example, since the end of the 2000s, China has placed restrictions on the use of American software, such as Google's tools, on its territory, including for Western companies located there, which greatly complicates their daily activities. More recently, the Russian invasion of Ukraine, since late February 2022, has led to an American offensive, and to a lesser extent a European one, against Russian software providers. Sanctions have targeted Kaspersky, a cybersecurity company whose antivirus software is widely used in Europe, to prohibit or advise against its use within the administration and companies in sensitive sectors.[20]

Open Source: An Essential Element of Software Development

Principles Underpinning Free and Open Source Software

In contrast to proprietary software, free and open source software is, in principle, without nationality and therefore without borders. The open source license model entails that users have access to the source codes of a software, allowing redistribution, modifications and additions, with much fewer restrictions than in the case of proprietary software.[21] Historically, the

17. U.S. Department of Commerce, "Commerce Implements New Multilateral Controls on Advanced Semi-conductor and Gas Turbine Engine Technologies", August 12, 2022, available at: www.bis.doc.gov.
18. M. Velliet, "Convaincre et contraindre : les interférences américaines dans les échanges technologiques entre leurs alliés et la Chine", *Études de l'Ifri*, Ifri, February 2022.
19. The Institute of Export & International Trade, "Cloud Computing and Export Control", September 9, 2020, video available at: https://youtu.be.
20. A. Guiton, "Face au russe Kaspersky, la défiance virale des Occidentaux", *Libération*, May 5, 2022.
21. Note that there are different types of open source licenses, more or less restrictive in the access to source codes and the use that can be made of them. Two models coexist. On the one hand, there are the reciprocal licenses (called "copyleft" in reference to the notion of copyright, such as the GNU General Public License, dating from 1989), which impose the sharing of the software under the same terms, and even of any improvement or software developed on its basis. On the other hand, there are the so-called

open source movement stems from the free software movement, born in the 1980s in the U.S. Open source software (OSS) is also widely used in research organizations, because of its adaptability and customizability to the needs of experiments.

Some open source software and components are of paramount importance for the development of many software and for the functioning of the Internet; they underlie the global software infrastructure, and are present in the software developed by private companies. Among them are the Python and Perl programming languages, the Linux operating system, the Mozilla Firefox web browser, the MySQL database management system, the Apache HTTP server, and most Java tools. Proof of the model's vitality, 10,000 lines of code are added to Linux every day, and 5,000 lines are modified daily.[22]

The Hybridization of the Free and Proprietary Models

Software publishers have long been reluctant to accept this model, which they consider to be contrary to the principle of intellectual property, on which their business model is based, with one Microsoft representative going so far as to describe OSS as "unamerican".[23] Now, starting the launch of Linux in 1991, the use of open source has increased sharply in recent decades and particularly from the 2010s.[24] Companies and governments both started including open source code in their products, to meet their specific needs. Companies also contribute to the development of OSS via their programming teams or by making internally developed programs available to the open source community (see below). As an illustration of this turnaround in the private sector, in 2008 Google launched the Android cell phone operating system, based on a modified version of Linux. This system is now dominant and 2.5 billion devices worldwide use Android.[25]

There is therefore both a complementarity and a convergence between proprietary software and open source software. We have seen that open source technological bricks are today integrated into almost all proprietary software developed by companies. The reality is therefore often a mixture of both models: software developers create assemblies of existing open source components and proprietary elements. According to one estimate, modern software applications often contain more than 100 open source components.[26] Generally, the lower levels of the system can be open, while the user interfaces, where the innovations in software and applications are

permissive licenses that allow the redistribution of the code under other licenses provided certain obligations are maintained (e.g., the Apache, MIT, etc. licenses).

22. K. Brigham, "How Open-Source Software Took Over the World ", *op. cit.*

23. *Ibid.*

24. European Union, "The Economic and Social Impact of Software", *op. cit.*

25. K. Brigham, "How Open-Source Software Took Over the World ", *op. cit.*

26. D. Geer *et al.*, "Should Uncle Sam Worry About 'Foreign' Open-Source Software? Geographic Known Unknowns and Open-Source Software Security", Lawfare, August 25 2022.

located, are proprietary. This creates what is called dependencies, and it is sometimes difficult to trace all the components of a software (see below).[27]

Second, "free software" does not necessarily mean "non-commercial software". On the contrary, a free program can be used, developed and distributed in a commercial context.[28] There are also so-called "commercial open source" software, such as those developed by Red Hat: the company develops products under an open source license and ensures its profitability by charging its customers for support, maintenance and installation.[29] In addition, venture capital funds are increasingly investing in open source software start-ups, and this sector has rather benefited from the acceleration of digitalization induced by the COVID-19 pandemic.[30]

Finally, there has been an evolution in the types of licenses used in open source. Copyleft licenses (such as the General Public License, GPL), whose concept was developed in 1985, offer freedom to "execute, copy, modify and distribute the computer code" and impose the maintenance of these freedoms in all versions derived from the software.[31] In other words, this type of license does not allow the creation of proprietary software based on copyleft source codes. However, large technology companies tend to deviate from these principles, such as Google, which developed Android based on Linux, but assigning it a non-copyleft license, thus freeing itself from disclosing the modifications of the source code made by Google.[32]

Open Source in Cloud- and Emerging Technologies

Finally, open source is now intrinsically linked to the cloud and plays a key role in emerging technologies (AI, edge, IoT). Open source components are indeed used in building cloud environments. If the infrastructure is not the element where the added value of the applications made available on the cloud is located, the interoperability offered by OSS makes it an essential element of the cloud architecture.[33] All cloud platforms are converging on Kubernetes, an open source container orchestration technology.[34] In turn, the cloud as a service has also shaped the growing development of open source.[35] According to Kevin Xu, cloud platforms have fundamentally

27. Federal Register, "Improving the Nation's Cybersecurity", *op. cit.*, p. 14.
28. GNU, "Qu'est-ce que le logiciel libre ? ", no date, available at: www.gnu.org.
29. T. Herr, "Responding to and Learning from the Log4Shell Vulnerability", *op. cit.*
30. Tech Crunch, "Where Top VCs Are Investing in Open Source and Dev Tools", February 5, 2020, https://techcrunch.com.
31. M. O'Neil *et al.*, "Le pillage de la communauté des logiciels libres", *Le Monde diplomatique*, January 20-21, 2022.
32. *Ibid.*
33. Interview, Sébastien Massart, Director of strategy, Dassault Systèmes, June 23, 2022.
34. K. Xu, "Open Source in China: The Trends", Interconnected, May 14, 2020, available at: https://interconnected.blog.
35. European Union, "The Economic and Social Impact of Software", *op. cit.*

changed the way open source technologies are distributed, so much so that the cloud can now almost be considered "an open source application store".[36]

Open source will also play a key role in the development of emerging technologies, including AI and IoT. Technological innovations and the new uses associated with them are leading to an explosion of software needs, and are also transforming the software industry ecosystem, since any type of company can now be involved in software development. As an example, there are now more lines of code in a car than in a F15 fighter plane.[37] And the number of these "smart" and interconnected devices continues to grow. For example, between 2010 and 2020, the number of connected IoT devices increased by about 1,000%; in 2020, they represented more than 50% of all connected devices.[38] IoT incorporates open source components for functions such as fleet management and embedded systems software platforms. For the French computer science research institute (Inria), as IoT becomes more widespread and system complexity increases, such software must be "general-purpose, open source, reusable across heterogeneous hardware and vendors, implementing a set of common standards and APIs."[39]

Moreover, AI and IoT, and more generally embedded software, pose particular risks in terms of system and personal security, as mentioned above. Therefore, according to Inria,

> "For states, the challenge is to minimize dependence on technical solutions which can be weaponized."[40]

Moreover, AI and IoT pose challenges in terms of ethics. Open source can then be seen as a way to supervise algorithms. As for AI, a report by the European Parliament in 2019 pointed to the need to include the public in the AI development process and, to do so, to "publish in open source all algorithms, tools and technologies funded or co-founded by the public" and to facilitate the auditing of source codes.[41] The report points out, however, that source code transparency does not prevent potential bias in the data, and acknowledges that disclosure of source code could potentially lead to misuse and manipulation of algorithms.[42]

36. K. Xu, "Open Source in China: The Trends", *op. cit.*
37. K. Brigham, "How Open-Source Software Took Over the World", *op. cit.*
38. Inria, "Internet of Things (IoT) : Societal Challenges & Scientific Research Fields for IoT", White Book, No. 5, 2021, p. 15.
39. *Ibid.*, p. 82.
40. *Ibid.*, p. 20.
41. European Parliament, "REPORT on a Comprehensive European Industrial Policy on Artificial Intelligence and Robotics", A8-0019/2019, January 30, 2019, available at: www.europarl.europa.eu, p. 45 and 18.
42. *Ibid.*, p. 26.

Victim of its Success? Challenges of and to Open Source Software

Cybersecurity Issues

Like all software, open source software presents specific cybersecurity challenges, mainly due to its ubiquitous nature: as pointed out in the introduction, about 80% of software contains open source components. There is a debate about whether open source is more secure than proprietary software, with one argument being that the accessibility of open code multiplies the chances of identifying vulnerabilities,[43] while the opposite argument is that the very large amount of open source code lines in the software can make it difficult to examine.[44]

Two major security breaches have highlighted the need for cybersecurity in open source bricks: the so-called Heartbleed vulnerability in 2014, and the so-called Log4Shell vulnerability in December 2021. The Heartbleed security vulnerability came from an error in the code of OpenSSL, a library of encryption tools. The error, present since 2012 was only discovered in March 2014 by Google's security team and Finnish engineers. Exploiting this vulnerability could expose encrypted content such as usernames, passwords, private keys, and data exchanged via these certificates.[45]. OpenSSL is used by about two-thirds of websites, including banking and e-commerce sites, and social networks. So while it is difficult to estimate the extent to which this vulnerability has been exploited by malicious actors, it has been described by many experts as one of the worst breaches in the history of the Internet.[46]

Other flaws can be introduced on purpose by malicious developers. In 2018, a GitHub contributor introduced a module into a code library used for bitcoin wallets, and used this module to introduce a backdoor and redirect funds to a server located in Kuala Lumpur.[47]

More recently, in December 2021, a vulnerability affected the Log4J logging software component (which records an application's activities), used in many applications and websites using the Java language. The vulnerability was identified by an engineer from the Chinese company Alibaba and disclosed by the Apache Foundation, which hosts the Log4J software. This vulnerability was likely to allow an attacker to take control of an application or even an information system. This time, the active exploitation of the

43. Linux Foundation and OpenSSF, "The Open-Source Software Security Mobilization Plan", *op. cit.*, p. 3.
44. Business Software Alliance, "Open Source and Commercial Software", *op. cit.*
45. "The Heartbleed Bug", updated on March 6, 2020, available at: https://heartbleed.com.
46. L. Ronfaut and B. Ferran, "'Heartbleed' : la faille qui frappe le cœur de la sécurité sur Internet", *Le Figaro*, April 11, 2014.
47. D. Goodin, "Widely Used Open-Source Software Contained Bitcoin-Stealing Backdoor", Ars Technica, November 26 2018, available at: https://arstechnica.com.

vulnerability has been proven[48] and attributed to "several groups of attackers, both state or state-related", operating in Russia, China, Iran and North Korea, as well as cybercriminals (botnets and ransomware operators).[49] Russia is suspected to have exploited this vulnerability to carry out cyber-attacks against Ukraine.[50] In turn, Log4Shell has been called "one of the most severe and widespread cybersecurity risks ever seen".[51] The developers of the project fixed the code error within two weeks after the vulnerability was identified.[52] However, to fix the vulnerability, previous versions of Log4J already installed must be updated, including many cases where users were not aware that this code was present in their own products.[53]

Finally, attacks against open source software are evolving. The year 2021 has seen a very large increase, estimated at 650%, compared to 2020.[54] In particular, the risk comes from a new generation of attacks, aimed at getting software developers to upload malware that takes the name of legitimate files, so as to infiltrate the upstream software supply chain.

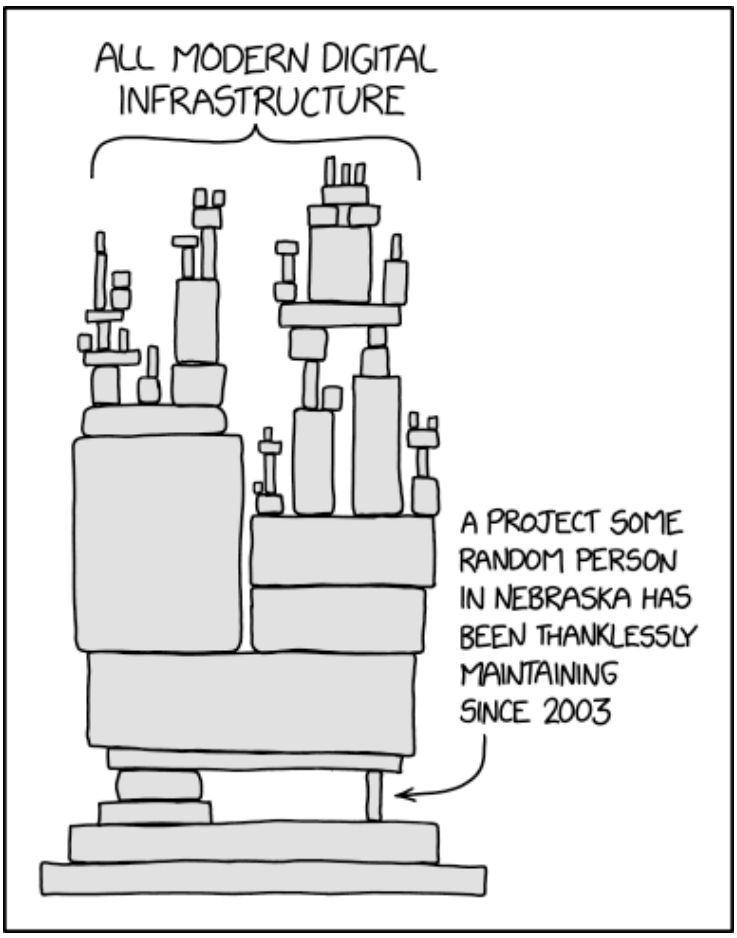
Issues of Economic and Technical Viability

As discussed in the previous section, proprietary software has security flaws, with equally deleterious consequences. Therefore, experts agree that Log4Shell and Heartbleed do not represent a failure of open source as such. However, in addition to their negative security consequences, these incidents have had the effect of highlighting the economic precariousness of the open source software model. Although some products are becoming popular to the point of becoming the backbone of the global digital architecture, these products rely for a large part on voluntary contributions from developers, who write, maintain and correct lines of code voluntarily. Note that this is not the case for the whole of open source, since there is now a profusion of code repositories, with paid or even full-time maintainers.[55]

48. ANSSI, "L'ANSSI alerte sur la faille de sécurité Log4Shell", Press communication, December 16, 2021, available at: www.ssi.gouv.fr.
49. "Log4j : 'Les experts s'accordent pour dire que la faille de sécurité est réellement inquiétante'", *Le Monde*, December 16, 2021. The main risk is concentrated on web servers. Many organizations may use Java tools and this Log4J library without necessarily being aware of them, for example if they do not know in detail all the tools on their network.
50. G. Peters, "Responding to and Learning From the Log4Shell Vulnerability: Opening Statement", Committee on Homeland Security and Government Affairs, United States Senate, February 8, 2022.
51. *Ibid.*
52. D. Nalley, "Responding to and Learning From the Log4Shell Vulnerability", *op. cit.*
53. R. Portman, "Responding to and Learning From the Log4Shell Vulnerability: Opening Statement", Committee on Homeland Security and Government Affairs, United States Senate, February 8, 2022.
54. Sonatype, "État de la chaine logistique logicielle", op. cit., p.4.
55. T. Herr, "Responding to and Learning From the Log4Shell Vulnerability", *op. cit.*

In the case of OpenSSL, the development team was very small and donations were becoming scarce.[56] Following the Heartbleed incident, the Linux Foundation pledged to financially support OpenSSL. This issue of underfunding, which had been raised as early as 2014, came back to the forefront following Log4Shell, to the point that states are now rallying, as we will examine in Part 3 of the report. In January 2022, a programmer himself sabotaged the code of projects he was working on to denounce the precariousness of the open source world.[57]

Figure 1: "Dependency"



Source: XKCD, August 16, 2020, available at: https://imgs.xkcd.com.

Furthermore, the precariousness of the current model does not reflect the economic value produced by open source software. According to a 2021 report, which examines the impact of open source software and hardware on the EU economy, this contribution is largely underestimated. The report estimates a positive impact of open source on the economy in the range of

56. K. Brigham, "How Open-Source Software Took Over the World", *op. cit.*
57. A. Horn, "Un développeur sabote son projet open source et paralyse des milliers d'applications", *Numerama*, January 10, 2022, available at: www.numerama.com.

€65-95 billion, for an annual investment (in 2018) of €1 billion in the EU. The report adds that an increase of 10% in contribution in open source would generate an increase in GDP in the range of 0.4% to 0.6%.[58]

For these reasons, both economic and security, there have been increasing calls to find sustainable solutions to funding open source. According to the European Union Intellectual Property Office (EUIPO), the system cannot be sustained without a mechanism to reward contributions to the common pool of knowledge.[59] The collaborative platform GitHub (see below) has launched a sponsorship program to allow developers to receive recurring donations for their work.[60] As we explain in the next section, the current trend is rather that of an increasing involvement of large tech companies in open source development, including through the acquisition of repository platforms. If they contribute to the economic health of the ecosystem, this trend may emanate from interests and practices that go against the very principles of open source.

Finally, the increasing centralization of open source around certain private actors can also become a weakness. On the one hand, in cases where large companies are directly involved in developing projects, there is a lack of organizational diversity in terms of contributors to these same projects, and a risk that if the company abandons a project, the entire open source community will lose out.[61] On the other hand, the centralization of the ecosystem around platforms, and the increasing involvement of states can lead to risks of changes to laws and statuses, which could repositories, codes, or licenses inaccessible to users from specific countries. In a recent example, Russian contributors working for Russian companies sanctioned in the context of the war in Ukraine had their GitHub accounts suspended.[62]

58. European Working Team on Digital Commons, "Towards a Sovereign Digital Infrastructure of Commons", report, June 2022, p. 20.
59. European Union Intellectual Property Office, "Open-Source Software in the European Union", Report, 2020, p. 25.
60. K. Brigham, "How Open-Source Software Took Over the World", *op. cit.*
61. G. Link, "Building and Supporting Open Source Communities Through Metrics", Open Source Summit Europe 2022, Dublin, September 13, 2022.
62. HackRead, "GitHub Blocks Accounts of Two Large Russian Banks Amid US Sanctions", April 16, 2022, available at: www.hackread.com.

Evolution of the Open Source Ecosystem: The Growing Influence of Big Tech

The global open source ecosystem relies on the contributions of developers, whether they are individuals, communities or companies. This ecosystem is structured around actors that host open source projects, organize and make accessible contributions to source code, bring together these actors, channel funds to contributors, and promote open source. Three types of organizations of various natures play structuring and evolving roles: foundations, code repositories and collaborative platforms, and large technology companies (the "Big Tech"). The latter are playing an growing role, as they are directly involved in open source projects, and they invest financially in foundations and code repositories. This can have potentially harmful effects on the open source model itself, due to the commercial interests at play, and risks of capture.

The Enablers of Open Source: Foundations and Collaborative Platforms

Foundations

Foundations play a key role in the governance, the structuring, and the activity of the open source ecosystem – in other words, they enable collaboration. More specifically, they have several functions: sharing information about OSS with private companies, neutral hosting for common assets, so that no one individually "holds the keys to the castle", legal personality and ability to receive money for projects, project infrastructure (servers, mailing lists, etc.).[63] Foundations' missions are more or less broad, depending on whether they focus on a programming language, a particular project (such as the Linux Foundation, in its early days, for the Linux project itself), or a domain (for example, infrastructure or cloud), or whether they are generalists (such as the Linux Foundation today).

The global open source ecosystem is today largely structured around a small number of mainly American foundations, of which we can mention the two main ones: the Linux Foundation (LF) and the Apache Software Foundation. The LF was set up in 2007 with the objective of promoting Linux and, increasingly, developing projects of commercial interest in various

63. T. Carrez, "The Role of Foundations", Open Source Summit Europe 2022, Dublin, September 15, 2022.

fields. Its mission today is to bring together large communities and investments, facilitate innovation, accelerate code development, ensure that code is written securely, and help manage intellectual property.[64] Currently, more than 100 projects fall under the umbrella of the LF, in sectors such as AI, autonomous vehicles, networks, or security.[65]

The Linux Foundation has 200 employees, and 1,000 members – companies that use open source technologies in their IT tools or in their products and services.[66] The Linux Foundation's revenue was $124 million in 2019 (rapidly growing from $15.6 million in 2011), coming primarily from conferences hosted by the foundation, fee-based services, as well as corporate membership fees, and training activities.[67] LF is involved in a growing number of large-scale projects, including support for other foundations and even the creation of foundations that are integrated within it, such as the Open Source Security Foundation (OpenSSF), created in 2020, or the PyTorch (machine learning) and OpenWallet (electronic wallet) foundations, which joined in September 2022. The motivation for PyTorch, the software developed by Facebook, to come under the responsibility of the Linux Foundation is that the latter has the required capacity to manage this project in which 2,400 contributors are involved.[68] If LF offers great visibility to the projects it supports, it is also accused of playing into the hands of big tech companies, at the expense of the community spirit of the beginning.[69] Some even call it "an industry consortium that organizes discussions between [the Big Tech]".[70]

Apache is the second largest American foundation. It has no employees but has 6,000 volunteers and a budget of about $2 million. The Apache httpd project, hosted by the Apache Foundation, is an HTTP server[71] which hosts one third of the world's websites. The Apache Foundation was created in 1999 to host this project and, since then, about 200 other projects[72]. Unlike LF, Apache members are individuals appointed based on their merit and their involvement in the foundation's projects.[73] That said, the foundation's main sponsors also include major tech companies (Microsoft, Apple, AWS, Huawei, etc.).

64. T. Krazir, "The Linux Foundation Became a Force in Enterprise Tech. Is That a problem?", Protocol, September 3, 2020, available at: www.protocol.com.
65. *Ibid*.
66. Linux Foundation, "Members", *op. cit*.
67. "Nonprofit Explorer: The Linux Foundation", ProPublica, no date, available at: https://projects.propublica.org.
68. I. Haddad, "Keynote", Open Source Summit Europe 2022, Dublin, September 14, 2022.
69. T. Krazir, "The Linux Foundation Became a Force in Enterprise Tech", *op. cit*.
70. D. Sabattier and L. Muselli, "Le logiciel libre, pillé par les Big Tech ?", verbatim account, February 1, 2022, available at: www.librealire.org.
71. HTTP: hypertext transfer protocol.
72. K. Finley, "For Open Source, It's All About GitHub Now", *Wired*, April 30, 2019, available at: www.wired.com.
73. Apache Software Foundation, "Members", no date, available at: www.apache.org.

Many other smaller or more specialized foundations exist. As we will see in the next section, the ecosystem is developing increasingly in Europe, especially with the relocation of the Eclipse and RISC-V foundations to the continent, and the creation in September 2022 of a European branch of the Linux Foundation.[74]

Collaborative Development Platforms and Code Repositories

In addition to foundations, the global open source ecosystem is increasingly structured around collaborative development platforms that host code repositories. As the use of OSS has become more widespread, communities of programmers have organized themselves and practices have become standardized around sites that host software projects and allow to collectively feed and manage source code.

GitHub is the main platform. Today, it has more than 60 million contributors worldwide,[75] versus 40 million in 2019.[76] The company, founded in 2008 in San Francisco, has become more popular as major tech companies – including Google, Facebook and Twitter – have chosen to host their open source project code there, and closed their own source code hosting services.[77] Microsoft did the same before it acquired GitHub for $7.5 billion in 2018. The quality and simplicity of the free interface also led the Apache Foundation to migrate all its projects to GitHub.[78] It is also the platform recommended by LF.[79]

For contributors, the fact that most projects are hosted on GitHub has certain advantages. The platform allows them to centralize their contributions, to build a resume and a network, and to receive sponsorships.[80] In addition, GitHub now performs many of the functions traditionally performed by foundations (project infrastructure, consulting, e.g. regarding licensing choices, managing payments to contributors).[81] However, it does not have the status of one. After its acquisition by Microsoft, many developers would have preferred to migrate to other repository platforms, but it has become difficult because of the centrality acquired by

74. Eclipse is a foundation mainly dedicated to industrial cooperation projects in areas such as cloud, edge, AI, connected vehicles, telecommunications and IoT. For its part, RISC-V is an open instruction set architecture for building a processor, originally developed at the University of California and available as open source...
75. GitHub, "Users", no date, available at: https://github.com.
76. K. Brigham, "How Open-Source Software Took Over the World", *op. cit.*
77. K. Finley, "For Open Source, It's All About GitHub Now", *op. cit.*
78. The Apache Software Foundation Blog, "The Apache Software Foundation Expands Infrastructure With GitHub Integration", April 29, 2019, available at: https://news.apache.org.
79. The Linux Foundation, "Starting an Open Source Project", no date, available at: www.linuxfoundation.org.
80. K. Finley, "For Open Source, It's All About GitHub Now", *op. cit.*; GitHub, "Sponsors", no date, available at: https://github.com.
81. T. Carrez, "The Role of Foundations", *op. cit.*

GitHub.[82] Another criticism of the platform is that the largest hosted projects are either developed or managed by large companies – individually or in consortia. As a result, the governance of these projects is not in the hands of the developers, but derives from industrial interests.[83]

The Growing Involvement of Large Technology Companies

Financing, Purchases and Contributions

As we have seen, the private sector has become a key player in the funding and governance of the open source ecosystem. Large digital companies, in particular, pay close attention to the vitality of the communities that develop and maintain these components, and invest significant resources in open source communities – either to ensure the continuity of the core software infrastructure, or to develop their own open source projects.[84] Thus, "in open source, fierce commercial rivals collaborate everyday".[85]

Most of the big tech companies are members or sponsors of the big foundations, which they finance: to be a platinum member of the Linux Foundation, it costs $500,000 per year. This is the case, among others, of Microsoft, Huawei, Ericsson, Intel, and Meta.[86] Support for OSS also includes the provision of technical resources to open source communities: after becoming a platinum sponsor of the Apache Software Foundation, Amazon has announced that it will also support the technical infrastructure on which the foundation operates.[87]

Big tech companies are also involved in open source through their developers, who contribute "massively" to projects hosted on GitHub.[88] They play a disproportionate role compared to other private players, according to the Open Source Contribution Index, which lists companies based on the volume of contributions their employees make on GitHub: Microsoft, Google and Red Hat are the top three contributors.[89] Thus, it is estimated that only 15% of Linux code is still produced by volunteers.[90]

82. M. O'Neil *et al.*, *The Coproduction of Open-Source Software by Volunteers and Big Tech Firms*, News & Media Research Centre, University of Canberra, 2021, p. 14.
83. *Ibid.*, p. 23.
84. European Working Team on Digital Commons, "Towards a Sovereign Digital Infrastructure", *op. cit.*, p. 23.
85. Brigham, "How Open-Source Software Took Over the World", *op. cit.*
86. Linux Foundation, "Members", no date, available at: www.linuxfoundation.org.
87. Z. Bhorat, "Supporting the Apache Software Foundation", AWS Open Source Blog, January 28, 2019, available at: https://aws.amazon.com.
88. M. O'Neil *et al.*, *The Coproduction of Open-Source Software*, *op. cit.*, p. 29.
89. Data dated September 2022. Open Source Contributor Index, available at: https://opensourceindex.io.
90. L. Muselli, "Les employés des GAFAM, plus gros contributeurs du logiciel libre", Polytechnique insights, June 8, 2021, available at: www.polytechnique-insights.com.

In some cases, Big Tech is directly involved in the structuring and management of the global open source ecosystem, through the purchase of companies or code repositories (as Microsoft did with GitHub). The desire to maximize this investment explains why Microsoft is by far the company whose employees contribute the most to the platform.[91] IBM, meanwhile, made its largest acquisition in 2018 when it bought Red Hat (13,000 employees, $2.4 billion in revenue) for $38 billion – the 3rd largest acquisition in U.S. tech history.[92]

Motivations of Big Tech Companies and Effects on the Ecosystem

What are the motivations for Big Tech companies to develop and make their software available under an open source license? This practice of open-sourcing can result from the obligations of certain licenses, if the project was itself developed on an open source basis. But, from another perspective, developing and/or making available in open source projects that companies could have carried out internally, is a choice. This choice of companies, and especially of tech giants, to use open source to develop their software is not obvious at first sight. Moreover, not all companies resort to open-sourcing - this depends on the company's strategy in terms of intellectual property, its culture and its relationship with open innovation, and their level of information about open source, how it works and who is involved.[93] Indeed, companies must weigh the benefits of sharing their codes and knowledge against the risks of losing control and differentiation from open source communities and potential competitors.[94] However, there are in fact multiple advantages to open source, which, on the whole, largely compensate for these risks, which is why open-sourcing tends to become increasingly widespread.

Saving Resources and Accelerating Innovation

The use of open source helps speed up the process and lower the costs of developing new software. On the one hand, using existing open source components means that companies do not have to start from scratch and "reinvent the wheel" when developing their products.[95] This is the main and original motivation for using open source.[96] But since open source is continuously fed by new projects, using it also allows access to new

91. M. O'Neil *et al.*, *The Coproduction of Open-Source Software*, p. 21.
92. Will Strategy, "Enquête sur l'état des lieux de la filière open source en France 2020/2021", Study Report, May 17, 2021, p. 8.
93. K. Blind *et al.*, "The Impact of Open-Source Software and Hardware on Technological Independence, Competitiveness and Innovation in the EU Economy : Final Study Report", European Commission, 2021, p. 37.
94. European Union Intellectual Property Office, "Open-Source Software", *op. cit.*, p. 26.
95. Portman, "Responding to and Learning From the Log4Shell Vulnerability", *op. cit.*
96. European Union Intellectual Property Office, "Open-Source Software", *op. cit.*, p. 25.

technologies that can then be adapted in a more refined and efficient way internally, by the companies.[97]

This motivation to use open source to accelerate software development and to innovate does not only concern digital companies and software publishers, but also companies from all sectors of industry since, as we mentioned in the introduction, software is now everywhere. Thus, large industrial and retail groups, such as Walmart, Exxon, or Mercedes Benz, use open source for this very reason.[98] Illustratively, in the automotive industry, major groups are working together in the Eclipse Foundation's Software Defined Vehicle Working Group to develop open and interoperable software modules for autonomous vehicles.[99]

In addition to saving time and accessing innovation, using open source reduces labor costs by saving the company developers' time. With no licensing and subscription costs, there are also savings on long-term software usage costs compared to proprietary solutions.[100] In doing so, open source lowers barriers to entry for companies wishing to enter the software development market.[101] In return, open source solutions developed by companies can also be monetized, by charging for support services, developing both open source and commercial versions, etc.[102]

Cybersecurity and Supply Chain Visibility

As mentioned, almost all software contains open source components as external dependencies. Knowledge of the components is necessary to comply with the legal obligations related to the different components of this software, but, more and more, the motivation is cybersecurity: open source components (as any software dependency) can create vulnerabilities, which can indirectly affect proprietary software developed by the companies.[103] It is therefore in their interest to develop knowledge or to contribute to the maintenance of the elements present in their supply chains.[104]

To mitigate these risks, major tech companies are investing directly in strengthening open source security. As an example, Google has taken several measures following Log4Shell, including a $100 million commitment to support dedicated organizations, such as the Open Source Security Foundation.[105] Google has also proposed establishing an organization that

97. Interview, Sébastien Massart, Director of Strategy, Dassault Systèmes, June 23, 2022.
98. K. Brigham, "How Open-Source Software Took Over the World", *op. cit.*
99. W. Gehring, "Drive Your Business Through Open Source Sponsorship", Open Source Summit Europe 2022, Dublin, September 13, 2022 ; Eclipse Foundation, "Software Defined Vehicle", no date, available at: https://sdv.eclipse.org.
100. European Union Intellectual Property Office, "Open-Source Software", *op. cit.*, p. 69.
101. *Ibid.*
102. K. Brigham, "How Open-Source Software Took Over the World", *op. cit.*
103. R. Portman, "Responding to and Learning From the Log4Shell Vulnerability", *op. cit.*
104. Linux Foundation and OpenSSF, "The Open-Source Software Security Mobilization Plan", *op. cit.*, p. 4.
105. K. Walker, "Making Open-Source Software Safer and More Secure", Google, January 13, 2022, available at: www.blog.google.

would serve as a marketplace for volunteer developers (tech company employees) to maintain the most critical open source projects.[106] In May 2022, Google created an internal team dedicated to this mission[107]. Finally, the company launched a program in August 2022 through which it will pay researchers to identify bugs in the latest versions of Google's open source software.[108] The amount of granted can go up to $30,000 per vulnerability found in the flagship programs of the company. For its part, Mercedes-Benz has chosen to financially support, via GitHub, contributors to open source projects that the car company considers the most important.[109]

Encouraging Product Adoption

While cost and supply chain visibility issues have long been paramount in the choice to use open source, tech companies now have more strategic motivations when they choose to deploy certain projects in open source. Open-sourcing aims in particular to encourage the adoption of products. Private players acknowledge these motivations: "We didn't [open source] to get help from the community, to improve the product. We did it as a freemium strategy, to encourage adoption", the director of the company that develops the MongoDB database management software explains.[110]

Encouraging adoption… or even creating standards: developing an open source solution makes it possible to create network effects, to maximize the chances that a solution will be used by others, and/or to weaken the position of another player already dominant in a market segment.[111] This is how we can explain why Apple opened Swift[112], and Meta, PyTorch. Moving proprietary projects to open source encourages engineers to develop applications based on these technologies, turning them into standards, thereby increasing the value and adherence to the Apple and Meta platforms.[113] As a result of such strategy, PyTorch is already considered "a leader in the [AI] market, with over 150,000 projects built on GitHub with PyTorch."[114] Following its transformation into a foundation, PyTorch is now

106. *Ibid*.
107. J. Lausson, "Google lance une petite équipe spécialisée dans la mise à jour du logiciel libre critique", Numérama, May 16, 2022, available at: www.numerama.com.
108. S. Gatlan, "Google Launches Open-Source Software Bug Bounty Program", BleepingComputer, August 30 2022, available at: www.bleepingcomputer.com.
109. W. Gehring, "Drive Your Business Through Open Source Sponsorship", *op. cit*.
110. Cited by D. Berkholz, "The Business of Open Source : How Big Money, Investors and Greed Are Changing Open Source Forever", Open Source Summit Europe 2022, Dublin, September 14, 2022.
111. European Union Intellectual Property Office, "Open Source Software", op. cit., p.25.
112. Swift is the programming language developed by Apple to develop applications compatible with Apple products (iOS, Mac…)…
113. K. Xu, "Open Source in China: The Game", Interconnected, May 10, 2020, available at: https://interconnected.blog.
114. S. Vaughan-Nichols, "Machine learning: PyTorch de Facebook passe sous le giron de la Fondation Linux", ZDNet, September 16, 2022, available at: www.zdnet.fr.

going so far as to offer free training to company executives, so that they can familiarize themselves with the tool.[115]

Companies' interest in developing sticky products, and the fact that they have an underlying interest in vendor lock-in, goes against the basic principles of open source and the ambition of interoperability.[116] Far from preventing companies, developers and users of software solutions from becoming captive to certain suppliers, the use of open source by large platforms can, in the end, prepare and facilitate this captivity in a pernicious way.

Developing the Workforce and Identifying Talent

Another motivation of the private sector concerns the identification of developers who, having demonstrated their abilities and involvement in open source projects, can then be recruited by companies.[117] Thus companies scan the profiles of contributors, especially those who contribute to their projects, and have developed specific skills that can be useful to them.[118]

Reputation

Finally, investment in OSS can be a marketing and reputational strategy, which can border on "open source washing". As summarized by a representative of the Zetta Venture Partners: "The beauty of open source from an investor's perspective is distribution, not innovation – it's contribution to marketing, not to [R&D]".[119] In the eyes of other companies and the public, open sourcing can counteract negative perceptions of dominant players, in that it can provide assurance that the company will not exercise excessive control over a given software product in the future.[120]

Another issue, especially with respect to public authorities, is the transparency of algorithms. As part of its "commitment to open science", Meta announced in May 2022 the sharing of the Open Pretrained Transformer (OPT-175B) program, with its 175 billion parameters trained on public data sets. Meta's goal is to facilitate "community engagement in understanding this fundamental new technology".[121] Despite the apparent effort at transparency – Meta's OPT-175B model is available upon request for

115. I. Haddad, "Keynote", *op. cit.*
116. D. Berkholz, "The business of Open Source", *op. cit.*; K. Xu, "Open Source in China: The Game", *op. cit.*
117. European Union Intellectual Property Office, "Open-Source Software", *op. cit.*, p. 25; Interview, Bruno Sportisse, CEO of Inria, July 13, 2022.
118. K. Xu, "Open Source in China: The Game", *op. cit.*; Interview, Bruno Sportisse, CEO of Inria, July 13, 2022.
119. Cited by D. Berkholz, "The Business of Open Source", *op. cit.*
120. European Union Intellectual Property Office, "Open-Source Software", *op. cit.*, p. 25.
121. S. Zhang *et al.*, "Democratizing Access to Large-Scale Language Models With OPT-175B", Meta AI, May 3, 2022, available at: https://ai.facebook.com.

research purposes – this program says nothing about the algorithms Meta uses on its Facebook and Instagram apps.[122]

So there is a tension between this façade of altruism and the desire to create value and product endorsement. This tension is summarized in a blog post from the Quai d'Orsay's digital diplomacy team, as follows:

> "The support of monopolistic actors for the development of open source technology bricks can be a way for [them to communicate] on their generosity and values. Because these bricks are then integrated into their finished products, which are themselves tightly locked and monetized. [...] these financing and buyouts are therefore both a strategy of image [...] - and of more or less subtle (re)enclosures".[123]

In short, the term "open source" tends to be hijacked for commercial interests.[124] More generally, we note that the motivations of private actors to invest in open source tend, in many cases, to diverge significantly from the philosophy behind OSS.

122. M. Heikkilä, "Inside a Radical New Project to Democratize AI", MIT Technology Review, July 12, 2022 ; Protocol Enterprise, "Facebook Opens an Algorithm; No, Not That One", May 3, 2022, available at: www.protocol.com.
123. B. Pajot, "Des barbelés sur la prairie Internet : contre les nouvelles enclosures, les communs numériques comme leviers de souveraineté", Diplomatie numérique, blog, July 31, 2020, available at: www.diplomatie.gouv.fr, p.5. We translate.
124. D. Berkholz, "The Business of Open Source", *op. cit.*

Governments Get Involved: (Geo)politicizing Open Source in the US, China and Europe

As mentioned, open source components are present in almost all proprietary software. Therefore, it is not surprising that the private sector is considered more "mature" than the public sector in understanding the role of open source in software supply chains.[125] The interest of governments in open source is not new. However, we are witnessing an evolution in their involvement, as governments are no longer only seeking to adopt open source or to develop software solutions through this means, but also to contribute to the financing or even the governance of open source ecosystems, at the national and/or global level. This involvement is not only pragmatic; it is increasingly politicized, whether it is to mitigate the risks of potential foreign interference in open source (as in the American case), to apply techno-nationalism and social control to open source communities, as in China, or to pursue a "third way" based on both the digital "commons" and "sovereignty", as in the European case[126].

United States: A Focus on Cybersecurity

Use of Open Source in the Federal Government

In the United States, open source related issues are primarily addressed from a cybersecurity perspective, and with a response focused on preventive measures within the federal government, and public-private cooperation.

A Desire to Generalize the Use of Open Source in the Administration

In the 1980s, the U.S. government relied primarily on custom proprietary software; the Department of Defense (DoD) was the largest buyer of custom software.[127] In the 1990s, there was a shift to purchasing off-the-shelf

125. European Working Team on Digital Commons, "Towards a Sovereign Digital Infrastructure", *op. cit.*, p. 23.
126. Other cases deserve to be studied further, in particular the Russian and Indian cases, because of the desire of both countries to develop alternatives to American and/or Chinese proprietary software. See in particular M.-G. Bertran, "La place des logiciels libres et open source", *op. cit.*; and K. Blind, *et al.*, "The Impact of Open Source Software", *op. cit.*
127. K. Blind *et al.*, "The Impact of Open-source software", *op. cit.*, p. 296.

software to reduce software development costs. At the same time, the 1990s marked the arrival of open source software in the infrastructure and backend of federal government IT systems. As the 2000s saw the U.S. private sector invest heavily in and promote open source (see above), the role of open source in DoD operations, and thus its importance to national security, grew. A 2003 report explains:

> "FOSS software plays a more critical role in the DoD than has generally been recognized. [For instance,] banning FOSS would remove certain types of infrastructure components [...] that currently help support network security. [As a consequence,] banning FOSS would have immediate, broad, and strongly negative impacts on the ability of many sensitive and security-focused DoD groups to defend against cyberattacks".[128]

While proprietary software has remained dominant, federal policy in the early 2000s encouraging consideration of software costs over time (including maintenance costs) and data protection has rather encouraged, but not openly recommended, the use of open source solutions.[129] In 2016, the U.S. government adopted a more assertive policy in favor of open source (the Federal Source Code Policy), thanks to a Memorandum encouraging the use within the federal government of open source solutions, the opening of source codes, and their reuse across various administrations, reserving off-the-shelf solutions as a second resort.[130]

A memo from the DoD Chief Information Officer (CIO), dated January 2022,[131] mentions that the use of open source by the government has several advantages: continuous peer review ensures software reliability and security to a greater extent than if a software is developed by smaller teams; the unlimited ability to modify source code allows the DoD to adapt quickly to changing situations and needs; open source reduces the risks associated with dependencies on proprietary software and the restrictions that can result (such as vendor lock-in); open source offers financial benefits when many copies of the software are needed, and for software maintenance; and open source is suitable for prototyping and experimentation.

Mitigating the Risks of Openness

However, OSS also presents challenges, particularly for the DoD, and for national security more generally. The first is that the use in critical systems of externally managed code potentially creates entry points for adversaries to seek to introduce malicious code into the DoD systems. The security of the open source software supply chain should therefore be subject to rigorous

128. T. Bollinger, "Use of Free and Open-Source Software (FOSS) in the U.S. Department of Defense", The MITRE Corporation, 2003, p.2, cited in *Ibid.*, p. 297.
129. *Ibid.*
130. *Ibid.*
131. Department of Defense, Chief Information Officer, "Software Development and Open-source software", Memorandum, January 24, 2022, available at: https://dodcio.defense.gov.

scrutiny. The Chief Information Officer's memorandum provides the following caveats for assessing the suitability of OSS for the DoD:

- **Long-term maintenance:** ensure that the software will be properly maintained by the open source community during its lifetime;
- **Trusted sources:** ensure that the software version comes from a trusted source, as there are many versions of the same software, some of which may be unreliable. To limit risks, the software should preferably be maintained by an established consortium or commercial entity;
- **Dependencies:** identify dependencies on sub-components on which the software is based;
- **Component security:** ensure the use of vulnerability detection tools by the developer community;
- **Component integrity:** risks are limited when codes are marked with digital fingerprints to guarantee the integrity of the code and ensure that it has not been modified;
- **Influence of foreign governments**: under U.S. law, open source is exempt from measures that apply to IT technology and service providers with obligations to foreign governments.[132] However, program managers should be aware of the potential influence of foreign governments on software. An audit of contributions to an open source project may be necessary to guard against malicious interference.

This last point is currently the subject of increased vigilance, as discussed below.

Finally, another challenge for the DoD stems from the fact that careless sharing of code developed for national defense systems could benefit adversaries by disclosing key innovations. Therefore, the Department must clearly articulate how, where, and when it participates, contributes, and interacts with the broader open source software community. The established principle is that the DoD can share the code it develops under an open source license, if it is not a component of "critical technologies".[133]

132. Public law 115-232, section 1655 (reference (I)), 2018.
133. Components of critical technologies are "information and technical data that advance current technology or describe new technology in an area of significant or potentially significant military application or that relate to a specific military deficiency of a potential adversary". Chief Information Officer, "Software Development and Open-source software", p. 6.

After Log4Shell: An Increasingly Geopolitical Approach

American concerns for the security of open source solutions have gone far beyond the DoD after the Log4Shell incident. Since the beginning of 2022, the White House and the U.S. Congress have paid increased attention to the broad and strategic functions of OSS and the risks that may be associated with it.

More Political Attention after Log4Shell

Already in May 2021, President Joe Biden signed an Executive Order (EO) on cybersecurity[134], following the SolarWinds attack (December 2020). In this document, where software is described as performing critical functions for the defense of the Nation's vital institutions, the White House called for increased cooperation with the private sector in identifying and sharing information about cyber threats, implementing enhanced cybersecurity practices and capabilities within the federal government (zero trust architecture,[135] vulnerability response procedures), and the examination of software supply chains. Specifically, the EO called for the use of tools, including automated tools, to review the provenance of software code and components, the widespread use of Software Bills of Materials (SBOMs),[136] and, in the case of open source software, "ensuring and attesting, to the extent practicable, to the integrity and provenance of open source software used within any portion of a product".[137]

The Log4Shell breach has led to a new round of policy initiatives, this time focused on open source. In January 2022, a meeting was held at the White House between the US Administration (Departments of Commerce, Defense, Energy, Homeland Security; Cybersecurity and Infrastructure Security Agency (CISA); National Institute of Standards and Technology (NIST)), major US tech companies (including Amazon, Apple, Google, IBM, Meta, Microsoft) and open source players (GitHub, Linux Foundation, OpenSSF),[138] to discuss the security of open source and its financing. The exchanges allowed to define three main objectives:[139]

134. Federal Register, "Improving the Nation's Cybersecurity", *op. cit.*
135. "The Zero Trust Architecture security model assumes that a breach is inevitable or has likely already occurred, so it constantly limits access to only what is needed and looks for anomalous or malicious activity. " *Ibid.*
136. The Software Bill of Material is the list of "ingredients" present in a software product, as these are for a large part the result of an assembly of open source and proprietary components. An SBOM allows to identify the presence of components or licenses that present risks or proven flaws.
137. Federal Register, "Improving the Nation's Cybersecurity", *op. cit.*, p. 7.
138. J. Lausson, "Log4j : la Maison-Blanche réunit le gratin de la tech pour discuter de la sécurité de l'open source", Numérama, January 13, 2022, available at: www.numerama.com.
139. Linux Foundation and OpenSSF, "The Open-Source Software Security Mobilization Plan", *op. cit.*, p. 5.

- Securing the production of open source software, with a focus on preventing security flaws and vulnerabilities in open source code and packages;
- Improve the processes of detection and correction of vulnerabilities;
- Shorten response time for patch distribution and implementation.

According to the Linux Foundation and the OpenSSF Foundation – the authors of the report that came out of the meeting – these efforts must be done in a public-private collaboration. The report says the public sector has a role to play in strengthening critical software infrastructures, including OSS supply chain, and proposes improved training for developers on security issues, and the creation of a public platform dedicated to analyzing the risks associated with open source components.[140]

The U.S. Congress has also initiated legislative work. The Senate held hearings in February 2022 to identify lessons to be learned from the crisis. The CHIPS and Science Act, passed in the summer of 2022, directs NIST to strengthen the security of open source software, disseminating information related to identified vulnerabilities, and producing voluntary guidelines to help entities that maintain code repositories discover and respond to vulnerabilities.[141] This measure is unambitious compared to what some members of Congress had proposed, including an amendment in the COMPETES Act bill, to create a series of centers of excellence for critical technologies, including one on open source. Such a center of excellence would have allowed public funding to be channeled directly into the open source projects and tools deemed most critical.[142]

Initiatives to strengthen the security of open source in the U.S. are still underway, however. On September 14, the government issued guidelines to limit the risk of vulnerabilities in software supply chains. These latest guidelines require software vendors to provide a self-certification (including the name of the software developer), or, in the case of open source products, to be evaluated by an organization certified by the Federal Risk and Authorization Management Program (FedRAMP).[143] At the same time, Senators Rob Portman and Gary Peters introduced a bill to "secure open source software", which intends to direct the federal Cybersecurity and Infrastructure Security Agency (CISA) to develop ways to review, assess and

140. *Ibid.*, p. 3.
141. United States Senate, "CHIPS and Science Act of 2022", Sec. 10224. "Software security and authentication. (a) Vulnerabilities in Open-source software".
142. W. Loomis and L. Wolff, "Defending Fire: A Need for Policy to Protect the Security of Open Source", Lawfare, February 8, 2022.
143. Executive office of the President, "Enhancing the Security of the Software Supply Chain through Secure Software Development Practice", Memorandum, September 14, 2022, available at: www.whitehouse.gov. In particular, FedRAMP provides approvals for cloud services.

mitigate the risks associated with open source components used by federal agencies.[144]

The Fear of Foreign Interference

The perception of risks related to open source is not only related to accidental vulnerabilities in components, but also and increasingly to the manipulation of codes by malicious actors potentially working for foreign governments. In order to better identify these risks of interference, the Defense Advanced Research Projects Agency (DARPA) announced in 2020 a project, called SocialCyber, which aims to:

> "explore capabilities to detect and counteract cyber-social operations that may target OSS developer communities[, such as] submissions of flawed code or designs, social media campaigns against OSS developers and maintainers critical of the flaws, as well as via misleading bug reports, obfuscating technical discussions and social capture of functional authority on OSS projects."[145]

Little information is available on how this project was implemented,[146] but it is interesting to note that open source is now approached as a domain in which adversaries can deploy actions not only of sabotage but also of disinformation.

This risk analysis is not geopolitically neutral. Indeed, there is a vocabulary coming from the White House and the DoD that suggests a geopoliticization of OSS, with references to national security, adversaries, and foreign interference. Four U.S. researchers and engineers have recently reported on officials' and civil servants' claims that certain open source components are avoided because of the contribution of Chinese or Russian individuals to their development, even when there are no security problems in the components:

> "We've heard anecdotes from a defense contractor that the web server NGINX – a popular software for storing and delivering web pages – has been banned from some government networks because one of the developers associated with the project is Russian."[147]

The researchers analyzed the nationalities listed on the GitHub profiles of the top 100 contributors to two structuring open source projects (Python and JavaScript packages). Only a fraction (less than 10%) of the open source contributors to these popular programs appear to be based in Russia or

144. T. Stark, "Senators Introduce a Bill to Protect Open-Source Software", *Washington Post*, September 22, 2022.
145. DARPA, "Hybrid AI to Protect Integrity of Open Source Code (SocialCyber)", DARPA-PA-20-02-07, no date, p. 2, available at: https://imlive.s3.amazonaws.com.
146. P. H. O'Neill, "The US Military Wants to Understand the Most Important Software on Earth", *MIT Technology Review*, July 14, 2022.
147. D. Geer *et al.*, "Should Uncle Sam Worry About 'Foreign' Open-Source Software?", *op. cit.*

China. The majority of contributors report being located in the United States or another country. Moreover, the number of contributors who did not indicate their geographical location exceeds 50% for some packages, making the analysis not very operational.

The authors further conclude that their research on software supply chain security does not suggest that knowledge of developers' geographic locations could have prevented the compromise of open source software. In other words, the data does not allow for a determination of whether Russian or Chinese developers are actually influencing open source software, or whether they are acting on behalf of their governments. However, U.S. officials' concern about this is likely to grow as-as we will see-Russian and Chinese developers invest in open source: the share of GitHub developers based in China increased by 15 percent between 2020 and 2021, and the share of developers based in Russia by 30 percent.[148]

China: Gaining Independence and Influence

Open Source Projects with a Global Reach

As mentioned, the share of Chinese contributors to global communities has been increasing significantly since the 2010 decade, and especially since 2020.[149] Between 2012 and 2018, the number of Chinese members of the Linux Foundation grew by over 400%.[150] Of the 73 million contributors to GitHub in 2021, 7.5 million were based in China, representing just over 10%, and the most represented nationality behind the US.[151] The Chinese open source community is therefore flourishing, and many GitHub projects developed by Chinese people have hundreds of contributors, thousands of forks[152] and have received thousands of positive evaluations.[153] It is notable that of the five most followed GitHub accounts in 2020, two were those of Chinese developers (but only one in 2022).[154] In March 2021, Alibaba, Huawei and Tencent were all in the top 20 GitHub repository contributions for the first time.[155] Among the influential projects is OpenResty. This API

148. *Ibid*.
149. B. Cameron Gain, "China's Open Source Activity Surged in 2020", devops.com, May 5, 2021, available at: https://devops.com.
150. R. Arcesati and C. Meinhardt, "China Bets on Open-Source Technologies to Boost Domestic Innovation", MERICS, May 19, 2021, available at: https://merics.org.
151. Z. Yang, "How Censoring China's Open-Source Coders Might Backfire", *MIT Technology Review*, May 30, 2022.
152. A fork refers to new software created from the source code of existing software.
153 K. Xu, "Open Source in China: Next Four Years", Interconnected, December 21, 2021, available at: https://interconnected.blog.
154. K. Xu, "Open Source in China: The Player", Interconnected, May 7, 2020, available at: https://interconnected.blog; GitHub, "Users", no date, available at: https://github.com.
155. B. Cameron Gain, "China's Open Source Activity Surged in 2020", *op. cit*. Contributions to GitHub are counted as the total number of forks, commits, stars, pull requests, issue comments and other metrics.

project[156] Gateway is one of the oldest Chinese open source projects, as it started in 2011, and the most used, as it is used by companies such as CloudFlare, Target and Lyft.[157]

Besides GitHub, there are also Chinese platforms, such as those founded by Tencent and Alibaba, and Gitee, the leading platform in China.[158] Gitee now has over 8 million users.[159] Some developers prefer to use Gitee rather than GitHub, for its better technical performance (due to the proximity of the platform's location, on Chinese territory) and the absence of risk of foreign interference (see below).[160]

According to the China Academy for Information and Communications Technology, about 87.4% of Chinese companies use open source technologies.[161] Like all digital companies in the world, they do this to develop their programs, increase the visibility of their projects and encourage adoption, attract talent, and more generally gain influence on the digital world.[162] Moreover, China's desire to become independent of American technologies is a growing motivation to use OSS.

As evidence of China's increasingly central place in the ecosystem, and its ambition to use OSS to develop critical technologies, one can mention several areas in which major Chinese companies are particularly invested: operating systems, semiconductors, cloud, and artificial intelligence.

Operating System

Huawei, a telecom networking, cell phone and cloud company, is a major contributor to, and clear beneficiary of, open source. The company, placed on a red list in 2020 by the U.S., is in fact the largest contributor to the kernel[163] of the Linux operating system, which is "the core building block of nearly all cloud computing, virtually every supercomputer, the entire internet of things, billions of smartphones, and more".[164]

Many parts of Huawei's own technologies rely on foreign contributions to open source software, chiefly Android. In May 2019, Huawei lost the operating license to use Google's Android system, following White House sanctions against the Chinese company. In return, Huawei has accelerated its plans to develop an alternative to Google's operating system, but also based on Android: Harmony OS. The ambition is not only to accommodate

156. API is the acronym for Application Programming Interface, which facilitates the interaction between several software programs, i.e. gives them access to the functionalities and services of other programs.
157. K. Xu, "Open Source in China: Next Four Years", *op. cit.*
158. Z. Yang, "How Censoring China's Open-Source Coders Might Backfire", *op. cit.*
159. *Ibid.*
160. *Ibid.*
161. R. Arcesati and C. Meinhardt, "China Bets on Open-Source Technologies", *op. cit.*
162. *Ibid.*
163. The kernel is a central component of some operating systems, which manages the computer's resources and allows the various components (software and hardware) to communicate with each other.
164. M. O'Neill *et al.*, "The US Military Wants to Understand", *op. cit.*

the restrictions imposed by the United States, but also to develop a competitor to the two dominant offerings, that of Google, and that of Apple (iOS) to conquer international markets, especially in Africa, where Chinese mobile terminals (including the Transsion brand) are already the most popular.[165] Finally, Huawei, with Harmony OS, is also targeting the 5G and IoT market.[166]

Semiconductors

In addition to operating systems for mobile devices, Chinese companies are also reliant on open source in the hardware and software used to manufacture semiconductors. China, through Alibaba and Huawei in particular, has invested alongside U.S. giants such as Google, and Europe's NXP in the RISC-V project community for open source semiconductor designs. RISC-V technology has been the subject of increased investment in China since 2018 via the "China RISC-V Alliance", composed of research institutes and companies.[167]

While RISC-V, as an open source project, does not fall under U.S. export restrictions, some in the U.S. have expressed concern that the project allows China to expand its semiconductor production ecosystem. A Congressional Research Service report suggests that platforms such as RISC-V allow Chinese companies and institutes of concern to the U.S. government to access U.S. hardware and software technologies and capabilities in what is considered a strategic area.[168] It should be noted that Europe is also seeking to develop its supercomputing capabilities on the basis of RISC-V[169]. In addition, the foundation, originally based in the United States, recently relocated to Switzerland to protect itself from potential future U.S. restrictions – a move that would seem to have positive consequences for Chinese users.[170]

Cloud

As explained above, the technological foundations of cloud computing are made up of open source building blocks. Due to the growth of cloud usage in China, Chinese companies are actively involved in the development of these technologies, especially through the Cloud Native Computing Foundation, which is part of the Linux Foundation.[171] According to a GitHub manager,

165. H. Tugendhat, "Huawei Is Trying to Avoid U.S. Sanctions. That May Change the U.S.-China Tech Rivalry in Africa", *The Washington Post*/Monkey Cage, April 30, 2021, available at: www.washingtonpost.com.
166. R. Arcesati and C. Meinhardt, "China Bets on Open-Source Technologies", *op. cit.*
167. C. Meinhardt, "Open Source of Trouble", *op. cit.*
168. K. M. Sutter, "China's Recent Trade Measures and Countermeasures: Issues for Congress", Congressional Research Service, Report R46915, December 10, 2021, p. 42.
169. R. Loukil, "Pourquoi Intel et l'Espagne investissent dans une nouvelle génération de microprocesseurs", *L'Usine Nouvelle*, June 9, 2022.
170. S. Nellis and A. Alper, "U.S.-bBsed Chip-Tech Group Moving to Switzerland Over Trade Curb Fears", Reuters, November 25, 2019.
171. K. Xu, "Open Source in China: The Players", *op. cit.*

Kevin Xu, China is the third largest contributor to these projects, behind the U.S. and Germany. Among the contributing companies, PingCAP (databases) and Huawei are the most active.[172] The latter is also "an active member and supporter" of the European cloud infrastructure project, Gaia-X – infrastructure that Huawei says it wants to help make "both extremely open and extremely secure".[173]

Artificial Intelligence

Finally, Chinese companies participate in open source projects in artificial intelligence. As explained above, the most widely used deep learning frameworks worldwide are Google's TensorFlow and Meta's PyTorch. In 2016, Baidu wanted to develop a Chinese alternative, with the deep learning platform PaddlePaddle. Since then, Huawei and XDL have also launched their platforms. At this point, however, the TensorFlow repository has eight times more contributions than PaddlePaddle.[174]

China is more successful in more specialized and emerging areas, such as AI for autonomous vehicles.[175] Baidu has had remarkable success with Apollo, an autonomous driving system. Chinese and European companies (BMW, Volkswagen) have joined the project.[176] So much so that Apollo could become, by 2025, the main open source alternative to Tesla's autonomous driving software stack, which is totally closed and proprietary.[177]

A Strong Involvement of the Chinese Government

A History of Government Involvement and International Collaborations

As open source takes center stage in the software solution development process, and becomes a sine qua non for innovation, Kevin Xu estimated in 2020:

> "China should embrace the open source way of doing things, like transparent governance, open discussions with stakeholders and developers, and fair procedures for rulemaking".[178]

In doing so, the country could reap the technological benefits of open source domestically, but also become a responsible international shareholder and a trustworthy player.[179] However, this is not the direction that the Beijing government seems to be taking. On the contrary, we are witnessing a growing

172. *Ibid.*
173. Huawei, "About Huawei Open Source", no date, available at: www.huawei.com.
174. R. Arcesati and C. Meinhardt, "China Bets on Open-Source Technologies", *op. cit.*
175. *Ibid.*
176. *Ibid.*
177. K. Xu, "Open Source in China: Next Four Years", *op. cit.*
178. K. Xu, "Open Source in China: The Players", *op. cit.*
179. *Ibid.*

involvement of the Chinese government in open source, which can be explained by economic and security interests, and a desire to gain independence from American technologies.[180] Originally, this involvement was done through international cooperative projects and participation in global open source communities, but it is increasingly translated into a nationalistic vision of OSS and a desire for state control over open source communities, thus going against the spirit and logic of open source.

The Chinese government's willingness to contribute to the development of open source is part of a broader strategy to become part of international collaborative networks to emancipate itself from dependence on American technologies, and to circumvent restrictions preventing China from acquiring certain technologies, for example by buying foreign companies. Thus, the effort in open source is accompanied by other initiatives, including the formation of joint ventures, research partnerships, programs to attract foreign talent, etc.[181]

The involvement of the Chinese government in open source is not new, already in 2007, Guohua Pan and Curtis Jay Bonk:

> "Unlike the spontaneity of open source movement in North America, open-source software development in China (...) is an orchestrated activity wherein different levels of China's government play a vital role in sponsoring, incubating, and using open-source software".[182]

Thus, the Chinese open source community emerged from the 2000s onwards from government initiatives, and largely in a context of international cooperation. One of the flagship projects was the Red Flag operating system, based on Linux, developed and distributed since 2000 by the Software Research Institute of the Chinese Academy of Sciences.[183] Then, the alliance for open source software was created in 2004, around Red Flag and in partnership with American companies such as IBM, Intel, and HP[184]. In the same year, China also launched a cooperation with France on the development of an open source infrastructure software stack (with CEA, Inria, Bull and STMicrolectronics)[185] and the establishment of an open source platform for middleware, called OW2.[186] OW2 still exists today, but has since become an independent and generalist foundation under French law.

180. Since the 2010s, the Chinese authorities have banned certain American software (the case of Google tools has been mentioned) for censorship purposes or for fear of spying risks. L. Whitney, "Microsoft, China Clash Over Windows 8, Backdoor-Spying Charges", CNET, June 6, 2014.
181. K. M. Sutter, "China's Recent Trade Measures and Countermeasures", *op. cit.*, p. 31.
182. G. Pan and C. J. Bonk "The Emergence of Open-Source Software in China", *International Review of Research in Open and Distance Learning*, Vol. 8, No. 1, 2007, summary.
183. *Ibid.*, p. 2.
184. D. Legard, "Open-Source Software Alliance Formed in China", NetworkWorld, August 11, 2004, available at: www.networkworld.com.
185. T. Gasperson, "France and China Sign Open Source/Open Standards Deal", Linux.com, October 11, 2004, available at: www.linux.com.
186. OW2, "Introducing OW2", no date, available at: www.ow2.org.

Towards a National Open Source Community?

In parallel to this movement of international interlocking and collaboration, however, there is a movement towards national open source technologies, which has gradually tended to strengthen.

As early as 2006, the Chinese government announced that all government agencies should use "locally produced software", an ambition that was to be achieved by 2010.[187] This type of argument has only become more prevalent (on both the Chinese and American sides) during the last decade, and even more so since 2020, as geopolitical tensions have increased and the desire to "decouple" has extended to new technological fields. Thus, today, according to the Chinese Academy of Sciences, although the country's participation in open source has increased, it remains insufficient, because the country is still too dependent on foreign foundations that support the global open source ecosystem.[188] Indeed, in light of the 2019 U.S. sanctions against Huawei, the Chinese government has begun to worry about its level of dependence on GitHub, owned by Microsoft.[189] And, in turn, because open source technologies are, by default, borderless, Chinese contributions are likely to be used by American tech giants.[190] Institutions with links to the Chinese governments therefore tend to use the Chinese platform Gitee.[191]

Accelerating U.S.-China competition has pushed strategic sectors of Chinese industry (banking, insurance, telecommunications) to adopt either domestic technologies or open source technologies, but preferably domestic open source technologies.[192] At the same time, the Chinese government's attention to, and desire for, control over open source has clearly increased since 2020. For fear of possible future US restrictions on the distribution of open source technologies (which are currently exempt from export controls),[193] China is banking on the development of national communities. The Iranian precedent where, in 2019, GitHub restricted access to its platform as a result of U.S. sanctions, had China fearing the worst.[194]

187. P. DeGroot, "Chinese PC Makers to Ship Legal OSs ", Directions on Microsoft, 25 December 2006 cited in Pan and Bonk "The Emergence of Open-Source Software in China", *op. cit.*
188. Y. Long *et al.*, "Development Experience of International Open Source and Its Enlightenment to Construction of Open Source Innovation System in China", *Bulletin of Chinese Academy of Sciences*, Vol. 36, No. 12, 2021.
189. Z. Yang, "How Censoring China's Open-Source Coders Might Backfire", *op. cit.*
190. K. Xu, "Open Source in China: The Trends", *op. cit.*
191. Z. Yang, "How Censoring China's Open-Source Coders Might Backfire", *op. cit.*
192. L. Y. Chen, "China's Biggest Startups Ditch Oracle and IBM for Home-Made Tech", Bloomberg, January 24, 2019.
193. The Linux Foundation, "Understanding US Export Controls With Open Source Projects", no date, available at: www.linuxfoundation.org ; "开源与美国出口管制" ["Open Source and U.S. Export Controls"], OSChina.net, August 12, 2020, available at: https://mp.weixin.qq.com.
194. R. Arcesati and C. Meinhardt, "China Bets on Open-Source Technologies", *op. cit.* Iranian developers' access to GitHub platform have been restored in 2021. N. Friedman, "Advancing Developer Freedom: GitHub Is Fully Available in Iran", GitHub blog, January 5, 2021, available at: https://github.blog.

China's first open source foundation, OpenAtom, was established in 2020 as a lesson learned from the Iranian case.[195]

In the wake of this, China's 14th Five-Year Plan 2021-2015, released in March 2021, is the first to mention open source as a national strategic priority.[196] As a result, the Ministry of Industry and Information has set the goal of "creating two to three open source communities with international influence" by 2025.[197] Along with the Ministry of Education, Huawei has recently been involved in disseminating knowledge about open source software to students in high schools and universities.[198]

However, Chinese ambitions to contribute to the global open source community are pitted against another ambition of the Chinese state, which is to further control the domestic developer community. Projects hosted on Gitee are regularly censored because they contain language (of a political or obscene nature) that violates Chinese laws.[199] But the control seems to have recently reached a new level. On May 18, 2022, all open source projects hosted on Gitee were locked and hidden from public view, without any warning to the developers behind the codes. Many suspect that the Chinese state forced Gitee to censor the codes.[200] In a statement, Gitee only said that from now on, all new code submissions would be manually reviewed before they could be officially published, and that projects already on the platform would also be temporarily made private for review.[201] In addition, Gitee now requires any visitor to create a user account in order to download source codes. The platform said it had no choice in the matter.

In addition, in June 2022, the *South China Morning Post* reported that the founder and chairman of ArcherMind Technology (sometimes considered the Chinese equivalent of the American Red Hat), Wang Jiping, had been detained as part of a "disciplinary investigation" about which few details are available.[202]

195. R. Arcesati and C. Meinhardt, "China Bets on Open-Source Technologies", *op. cit.*
196. Y. Long *et al.*, "Development Experience of International Open Source", *op. cit.*; CSET, "Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035", May 13, 2021, available at: https://cset.georgetown.edu.
197. K. Xu, "Open Source in China: Next Four Years", *op. cit.*; Ministry of Industry and Information Technology of the People's Republic of China,"十四五"软件和信息技术服务业发展规划》解读 ["Interpretation of the Software Services and Information Technology Industry Development Plan 14th Five-Year Plan"], November 11, 2021, available at: https://www-miit-gov-cn.translate.goog. [Automatic translation.]
198. Huawei, "About Huawei Open Source", no date, available at: www.huawei.com.
199. Z. Yang, "How Censoring China's Open-Source Coders Might Backfire", *op. cit.*
200. *Ibid.*
201. Zihu.com, "如何看待 5 月 18 日 Gitee 仓库开源须审核，已开源部分仓库暂时关闭，审核通过后再次公开？" ["What do you think about the fact that the Gitee warehouse open source is scheduled to be reviewed on May 18, and that some warehouses that were open source are temporarily closed, and will be made public again after the review is passed"], discussion thread, available at: www.zhihu.com. [Automatic translation.]
202. J. Li, "China's Answer to Open-Source Software Giant Red Hat Says Its Boss Was Taken Away for Disciplinary Investigation", *South China Morning Post*, June 8, 2022.

China's nationalistic approach to open source has many limitations. On the one hand, existing open source technologies, such as RISC-V, are not sufficient to ensure that China will be able to compete with U.S. chips or fill the gaps created by restrictions on technology transfers.[203] On the other hand, the desire to create an indigenous ecosystem isolated from the international community could be detrimental to the quality of the software developed and the possibility that it will find an international market. Finally, it is obvious that this attitude of closure and censorship goes against the fundamental principles of open source.

Europe: Open Source, a Tool for the "Third Way"?

Digital Sovereignty and Promotion of the "Commons"

The European vision of OSS, and the political initiatives underway, are based on the historical role of Europeans in open source, the notion of "digital commons" in which open source is partly embedded, and the ambition of a European digital sovereignty, to which OSS contributes.

Europe in OSS: A Historical Role and a Steady Participation

Europe, along with North America, has played a pioneering role in free and open source software. For example, in 1993 the European Organization for Nuclear Research (CERN) put the web protocol, invented by British researcher Tim Berners-Lee, in the public domain, and released the next version under a free license, thus contributing to the emergence and diffusion of the Internet.[204] It is also worth noting that the founder of Linux, Linus Torvald, is Finnish and developed the project when he was a student in Finland. Because of these pioneering roles, North America and Europe numerically dominated the open source world until the 1990s, after which the geographical diversity of contributors increased.[205]

Today, European developers' contributions represent a little less than a third of the global open source communities. The MERICS institute estimates that Europe represents 26.8% of contributions to the GitHub platform, behind North America (34%) and Asia (30.7%). At the national level, still according to MERICS, the United States contributes the most (22.7%), ahead of China (9.67%) and India (5.2%).[206] Open source

203. R. Arcesati and C. Meinhardt, "China Bets on Open-Source Technologies", *op. cit.*
204. CERN, "La naissance du Web", no date, available at: https://home.cern/fr.
205. D. Rossi *et al.*, "Geographic Diversity in Public Code Contributions: An Exploratory Large-Scale Study Over 50 Years", The 2022 Mining Software Repositories Conference, Pittsburgh, May 2022, available at: https://hal.archives-ouvertes.fr.
206. R. Arcesati and C. Meinhardt, "China Bets on Open-Source Technologies", *op. cit.*

communities in Europe are particularly strong in Romania, the Czech Republic, France, Germany, and the United Kingdom.[207] For its part, a 2021 EU report ranks Germany, the United Kingdom and France in the top three positions, in terms of commits[208] and number of contributors on GitHub.[209]

A report from the EU Intellectual Property Office shows involvement in and use of open source among European technology companies stable (54-60% of respondents) or increasing (22-26% of respondents), during 2018-2020.[210] Forty percent of companies surveyed report having employees who develop open source programs on their work time.[211] According to the same report, the main reason why European software companies decide not to use open source (in the development or use of software) is the governance model of OSS, which they believe does not guarantee the sustainability of product development, which could harm their business model in the future.[212]

It is worth noting that while European companies do use and contribute to open source, they contribute on a smaller scale than their American and Chinese counterparts. For example, in 2022, only two European software companies, Germany's SAP and SUSE, are in the top 20 contributors to GitHub.[213] The authors of a report commissioned by the European Commission also note that:

> "In the EU, it is employees of small and very small businesses that are most likely to contribute OSS code ("commits") whereas in the US commits are mostly made by large ICT companies, which base their relevant business models successfully on the large body of freely available and continuously improving OSS code".[214]

However, European contributors are numerous. Today, the Linux Foundation estimates that 31% of its members are European.[215] To reflect this strong involvement, and the leading role of the EU, as a supranational actor, in promoting open source and international standards in the digital world (such as the RGPD), the foundation announced in September the creation of Linux Foundation Europe (LF Europe), which will be based in Europe.

207. J. Zemlin, "Keynote", Open Source Summit Europe 2022, Dublin, September 14, 2022.
208. A commit is the recording of a change to a code or file, in the context of a version control system.
209. Will Strategy, "Enquête sur l'état des lieux de la filière open source en France 2020/2021", Study report, May 17, 2021, p. 8.
210. European Union Intellectual Property Office, "Open-Source Software", *op. cit.*, pp. 37-40.
211. *Ibid*, p. 74.
212. *Ibid.*, p. 40.
213. According to the Open Source Contributor Index, available at: https://opensourceindex.io. In August 2022, there are two European companies in the top 20 (SAP, No.10, and SUSE No.16), three Chinese companies (Huawei, Tencent and Alibaba, respectively, 12th, 13th and 15th contributors), and 15 American companies in the top 20.
214. K. Blind *et al.*, "The Impact of Open-Source Software", *op. cit.*, p. 15. This observation is shared in the report of the European Union Intellectual Property Office, "Open-Source Software", *op. cit.*.
215. J. Zemlin, "Keynote", *op. cit.*

Preserving the "digital commons"

The European ambition in the digital world, in its values and its historical heritage, can be brought closer to the imaginary of the "digital commons". Indeed, preserving the digital commons would mean "preserving the original vision of the Internet, a diversified, non-monopolistic and non-privatized Internet"[216] promoted by Europe. More precisely, Europe and the digital commons share, according to French diplomacy, certain objectives: preservation of the general interest, free competition, net neutrality, protection of personal data, and ecological sustainability.[217]

It is important to distinguish open source from the digital commons. The latter are more ambitious since they overlap with the notions of collaborative governance, open data, free software and open standards.[218] The *libre* vision and principles are still defended by open source communities, and by small digital companies, but they have not been respected by the big technology groups.[219] According to commons advocates, these principles are undermined by the "enclosure strategies" of other states and large corporations.[220] Thus, while all commons are based on open code and/or data, not all open source components are "commons", depending on the licensing strategies of companies.

Commitment to *libre* principles and the commons also leads to reluctance in North American open source communities due to the penetration of the digital industry. *Libre* activists regret Microsoft's takeover of GitHub[221] and encourage the use and support of other alternative collaborative platforms, as suggested in a recent article signed by French open source actors.[222] Within the French government, this vision is carried by the Ambassador for Digital, Henri Verdier, who summarizes the issues as follows:

> "The more you have free resources, open source software, the more you build your economy on digital commons, the freer you are, because no one can expropriate you, nor change the prices, nor impose to you technological choices. [That is why we introduced the notion of "commons" in the debate.] We know that sometimes you can have predatory strategy, a capture strategy, through open source. Open source alone is not enough. If I open the source of my code but I control the commits, I'm still the master of the ecosystem and I control the ecosystem". [223]

216. Médiapart, "Pour que les communs numériques deviennent un pilier de la souveraineté numérique européenne", June 20, 2022, available at: https://blogs.mediapart.fr.
217. B. Pajot, "Des barbelés sur la prairie Internet", *op. cit.* p. 4.
218. European Working Team on Digital Commons, "Towards a Sovereign Digital Infrastructure", p. 2.
219. M. O'Neil *et al.*, "Le pillage de la communauté", *op. cit.*
220. Médiapart, "Pour que les communs numériques", *op. cit.*
221. M. O'Neil *et al.*, "Le pillage de la communauté", *op. cit.*
222. Médiapart, "Pour que les communs numériques", *op. cit.*
223. H. Verdier, "Open Source: Driving the European Digital Decade", Open Forum Europe, Conférence, Brno (Czech Republic), September 16, 2022, available at: www.youtube.com (minute 51').

Some European projects are giving concrete expression to this ambition to preserve the commons. The French National Institute for Research in Digital Science and Technology (Inria), with the support of UNESCO, is behind the Software Heritage project, launched in 2016. The goal of the project is to collect all publicly available software in source code form with its development history, to replicate it massively to ensure its preservation, and to share it with all those who need it.[224]

Open Source as a Tool for European Digital Sovereignty

The renewed political interest in open source in Europe is linked, in parallel, to the declared ambition to build European digital sovereignty. At the heart of technological infrastructures, and therefore of this sought-after sovereignty, are software and technological standards.[225] The creation of "open and shared software and hardware infrastructures as global digital commons" is presented as the fourth pillar of the European technological sovereignty project, alongside the securing of cyberspace, the legal and economic regulation of the digital market, and the European capacity for innovation.[226] Digital sovereignty is supposed to allow Europe, in the face of growing tensions between the United States and China "bringing shortages and a possible technological decoupling between the two blocks", "to ensure its autonomy while avoiding a forced and unconditional alignment".[227] The refusal to be forced to align explains why open source software- and hardware solutions are notably pursued and promoted by Europe in response to sanctions and restrictions on technology trade.[228]

According to Bruno Sportisse, CEO of Inria, for open source to be more than just an ideology, to contribute directly to digital sovereignty and industrial policy, and to create economic value, it must be supported by private companies.[229] In fact, in addition to the economic benefits of OSS for companies that we have discussed in the previous case studies, European companies also justify the use of and contribution to open source based on political arguments. For example, a representative of the German software company SAP gave the example of contact tracing applications at the beginning of the COVID-19 pandemic: the use of open source solutions was a way for the company to ensure the transparency of the technological

224. Software Heritage, "FAQ", no date, available at: www.softwareheritage.org.
225. S. Rolland, "'Il n'y aura pas de souveraineté numérique européenne sans maîtrise du logiciel', Bruno Sportisse, Inria", *La Tribune*, February 22, 2022.
226. French Presidency of the Council of the EU, "Conférence 'Construire la souveraineté numérique de l'Europe'", February 5, 2022, available at: https://presidence-francaise.consilium.europa.eu.
227. T. Breton, "Géopolitique technologique: il est temps pour l'Europe de jouer ses cartes", Blog, European Commission, October 11, 2021, available at: https://ec.europa.eu.
228. N. Flaherty, "European Processor Project Shows Shift to RISC-V", EE News Europe, December 23, 2021, available at: www.eenewseurope.com.
229. Interview, Bruno Sportisse, CEO of Inria, July 13 2022.

solution and thus gain public trust.[230] SAP also announced in September 2022 that it would be an inaugural member of the Linux Foundation Europe, justifying this participation as contributing to "European sovereignty".[231] In the same vein, the engineering software publisher and cloud provider Dassault Systèmes (or 3DS), in partnership with Netframe (collaborative workspace) and Nexidi (open source software publisher), have entered into a partnership for a joint software offering in the edge and the cloud. Their press release highlights the control of all technological bricks in Europe and an offer "compatible with the emergence of the Splinternet and resilient to geopolitical disruptions, such as economic sanctions on export markets" based on a "sovereign open source base".[232] Similar arguments have been made regarding open source in hardware, insofar as Europe, like China, relies on the open architecture of microprocessors, RISC-V, to develop its semiconductors.[233]

How is it possible to generalize the use of open source in the private sector and contribute to this ambition of sovereignty through open source? From the point of view of French representatives, Europe must be able to replicate the successes of open source internationally, such as the Chinese Appolo software for autonomous vehicles, which was developed more rapidly than Tesla's systems.[234] There are also economic arguments in favor of a greater use of open source in European industry. OSS represents a positive economic impact to the EU GDP estimated between €65 and €95 billion for the year 2018, for a total of €1 billion invested by companies.[235] The European Commission report, quoted above, also estimates that if the contributions of European companies to open source grew by 10%, this would potentially increase the EU's GDP by €100 billion, and create 1,000 digital businesses per year.[236]

A Growing Mobilization of the EU and Member States

Because of European objectives, which are related to the preservation of the "commons" and the quest for digital sovereignty, European states and the European Union are increasingly determined to adopt open source, develop open software, ensure the cybersecurity of these solutions, and finance the ecosystem. As previously indicated, OSS, in the strategies of large tech

230. V. Chandrasekhara, "Keynote: How Can the LF Enable Europe to Collaborate Locally and Innovate Globally", Open Source Summit Europe 2022, Dublin, September 14, 2022.
231. *Ibid.*
232. Netframe, "A l'occasion de Vivatech, la startup netFrame s'associe avec Dassault Systèmes et Nexedi, ainsi que Docaposte comme partenaire technologique, pour proposer une suite collaborative souveraine sur l'infrastructure cloud de confiance et souveraine 3DS OUTSCALE", press release, June 13, 2022.
233. C. Meinhardt, "Open Source of Trouble: China's Efforts to Decouple From Foreign IT Technologies", Merics, May 18 2020, available at: https://merics.org.
234. Interview, Project officer to the Ambassador for Digital Affairs, July 18, 2022.
235. K. Blind *et al.*, "The Impact of Open-Source Software", *op. cit.*
236. *Ibid.*

companies, can be a tool for gaining market share, and animating open source communities can serve marketing purposes. In fact, the major structuring foundations, which play a role in its ability to achieve "digital sovereignty", are American. This raises a series of practical questions: how to get involved in the governance of these organizations and in the development of codes, how to finance foreign projects, or how to attract foreign developers. As a result, Europe may find itself powerless to act when faced with players based abroad.

Adopting Open Source in Government and Public Services

European countries top the Open Data Barometer and Open Knowledge Foundations' Global Open Data Index.[237] The main line of action of European public authorities (at the level of member states as well as the EU) has been to develop the use of open source within administrations in response to their needs, and to open the codes and data produced by public institutions.

In France, the government's involvement in the adoption of open source solutions within administrations has increased in recent years. The narrative in favor of using open source is based on the issues of transparency and democracy, open science and innovation, and quality of public action.[238] In 2020, a report overseen by Senator Éric Bothorel and submitted to the Prime Minister recommended the creation of an Open Source Program Office (OSPO) in France, similar to what exists in a growing number of governments and companies.[239] Shortly thereafter, in April 2021, a circular from Prime Minister Jean Castex – the first on the subject since 2012, which had placed France "at the forefront" of data and source code policy in Europe – made free software and open data a "strategic priority of the state".[240] The ambition was to strengthen the opening of source codes and public algorithms, as well as the use of free and open source software within the administrations.[241] In June 2021, deputy Philippe Latombe published a report on digital sovereignty suggesting to impose within the administration the systematic use of free software, by making the use of proprietary solutions an exception.[242]

237. European Working Team on Digital Commons, "Towards a Sovereign Digital Infrastructure", *op. cit.*, p. 10.
238. Gouvernement, "Mission Bothorel – Pour une politique publque de la donnée", December 2020, p. 6.
239. *Ibid*. An OSPO is a team that oversees the strategy of an entity (government, company) in open source (needs, contributions, licensing issues, reuse of components...).
240. Systematic, "Politique publique de l'open source en France : 2021, une année pleine de promesses", January 2, 2022, available at : https://systematic-paris-region.org.
241. *Ibid*.
242. Assemblée nationale, "Bâtir et promouvoir une souveraineté numérique nationale et européenne", Rapport d'information, No. 4299, June 29, 2021, p. 139.

In September 2021, Departmental Data, Algorithm and Source Code Administrators (DDAAs) were appointed in all departments,[243] and an "Action Plan for Open Source software and Digital Commons" was developed and launched in November by the Minister of Transformation and Public Service, Amélie de Montchalin.[244] The action plan, which relies on an investment of €30 million, aims in particular to disseminate knowledge and use of free software and digital commons in the administration; and to enhance the value of public contributions to projects and open source communities.[245]

For its part, the European Commission updated and expanded its open source strategy in 2020, linking it to the ambition of "digital autonomy". As a result, the Commission created an OSPO whose role is to facilitate the implementation of the strategy and its action plan.[246] While the OSPO was established in 2020, it did not meet in person until September 15, 2022, on the sidelines of an event in Brno as part of the Czech Council Presidency. At the same event, the European Commission's Directorate General for Informatics (DGIT) announced the launch of a repository platform for European institutions to host about 100 projects and share open source solutions developed by the Commission.[247]

(Co-)developing Open Source Software

As explained in the American and Chinese cases, the public sector does not only use open source software solutions, but also develops such solutions – either to meet the needs of the administration or, in a public-private partnership approach, to contribute, through public funding and research, to co-develop open source solutions for industry and the private sector. Again, examples can be drawn from the French case, where the state, in partnership with companies, is developing open source solutions for critical software bricks in various emerging fields, such as AI, data analysis, and IoT.

Inria has developed Scikit-learn, an open source artificial intelligence toolkit for data analysis. Scikit-learn is one of the main world-class data science solutions, competing with PyTorch (Meta) and Tenserflow (Google).[248] The French company Data Iku, one of the leading French AI companies now headquartered in the United States, has developed its

243. Gouvernement, "Données, algorithmes et codes sources : une mobilisation générale sans précédent, à travers 15 feuilles de route ministérielles", September 27, 2021, available at: www.numerique.gouv.fr.
244. Gouvernement, "Plan d'action logiciels libres et communs numériques", updated on November 16, 2022, available at: www.numerique.gouv.fr.
245. Systematic, "Politique publique de l'open source en France", *op. cit.*
246. European Commission, "Open-Source Software Strategy 2020-2023", October 21, 2020, available at: https://ec.europa.eu; European Commission, "EC Open Source Program Office", no date, available at: https://joinup.ec.europa.eu.
247. A. Thévenet, "The European Commission Announces code.europa.eu at OFE Event in Brno", Open Forum Europe, September 23, 2022, available at: https://openforumeurope.org.
248. S. Rolland, "Il n'y aura pas de souveraineté numérique européenne sans maîtrise du logiciel", *op. cit.*

business from Scikit-learn.[249] Inria's ambition is to encourage other companies to develop digital tools based on the French Scikit-learn solution, rather than on American solutions.[250]

Another open source solution project in AI is the multilingual natural language processing project, BLOOM (for BigScience Large Open-science Open-access Multilingual Language Model). This project, trained on the French supercomputer Jean Zay, was officially launched in July 2022.[251] One thousand volunteer researchers participated in the BigScience project, co-funded by the French government and the open source AI platform, Hugging Face.[252] Unlike other large language models, such as OpenAI's GPT-3 and Google's LaMDA, which are proprietary solutions and whose code and AI models are closed, BLOOM is intended to be responsible and transparent. The researchers will share details about the data on which the model is trained, the challenges encountered in its development, and the evaluation of its performance.[253] The program can be downloaded on the Hugging Face website.[254] Another specificity is that the model is trained on multilingual data, and is currently able to generate text in 46 different languages.[255]

Ensuring the Cybersecurity of Open Source

Concerned about the security of open source software, in 2016 the EU set up a software audit pilot project, FOSSA (Free and Open source software Auditing), based on an initiative by the European Parliament following the Heartbleed breach.[256] In this context, the EU has organized bug bounties (financial rewards offered to individuals who identify and report bugs and flaws in software) for open source solutions used by the European institutions, as well as hackathons, meetings of developers aimed at collectively identifying solutions to common problems.

The EU currently provides €200,000 for its bug bounty program, with rewards of around €5,000, to engineers who identify flaws. Usually the bug bounties are organized by companies, including large U.S. technology companies, so there is "a real economic competition" around security flaws.[257] Therefore, the amounts proposed by the EU may seem "modest"

249. Interview, Bruno Sportisse, CEO of Inria, July 13, 2022.
250. *Ibid.*
251. E. Gibney, "Open-Source Language AI Challenges Big Tech's Models", *Nature*, June 22, 2022, available at: www.nature.com; A. Vitard, "Un millier de chercheurs ont développé un modèle de langue multilingue en open source", *L'Usine Digitale*, July 13, 2022, available at: www.usine-digitale.fr.
252. M. Heikkilä, "Inside a Radical New Project to Democratize AI", *op. cit.*
253. *Ibid.*
254. Hugging Face, "Bloom LM Version 1.0", May 26, 2022, available at: https://huggingface.co.
255. "Introducing The World's Largest Open Multilingual Language Model: BLOOM", BigScience Blog, no date, available at: https://bigscience.huggingface.co.
256. European Commission, "EU-FOSSA 2 - Free and Open-Source Software Auditing", no date, available at: https://ec.europa.eu.
257. "Log4j", *Le Monde*, *op. cit.*

compared to the amounts these companies can offer to secure proprietary software.[258]

The FOSSA initiative was followed by the FOSSEPS pilot project, launched in 2021, which continues the bug bounties, and conducts broader work, to identify the most critical open source software used in European public services, and to create an inventory to identify European dependencies in open source components that "may be in a critical state of health – i.e., software in danger of shutting down, software updates in progress, and bug fixes".[259] The inventory and the entire methodology used for the analysis of dependencies have been made public by the EU.

Inventory processes are also being put in place at the level of the member states. In June 2022, a three-year partnership was signed between ANSSI and CEA, to implement new approaches to verify the absence of vulnerabilities in software during the design and integration phases. To do this, the CEA and ANSSI teams will use an automatic code analysis platform, Frama-C, developed by the CEA and Inria and published in open source, which enables the exhaustive detection of a class of software vulnerabilities and "the evaluation for certification of security products at the most demanding levels".[260]

Finally, the European Union passed the Cyber Resilience Act in September 2022. This law, which deals with cybersecurity as a whole, provides for the implementation of an equivalent of Software Bills of Materials (SBOMs), requiring software vendors to identify and document the components contained in their products.[261] These lists will not be required for programs released under a non-commercial free license. However, these lists will necessarily identify open source components, since they are present in almost all software, including proprietary software.

Funding Open Source

European public actors (states, EU) are increasingly involved in open source, whether to generalize its use in administrations, (co-)develop software solutions, or work on the cybersecurity of computer systems. Another means of action by the public authorities in OSS concerns the financing of the ecosystem, in order to support it, help it develop, and ensure its maintenance. Here, too, there is a shift towards greater involvement of the EU and the member states.

258. J. Lausson, "LibreOffice, Mastodon : l'UE offre 200 000 € pour sécuriser certains logiciels libres", Numérama, January 24, 2022, available at: https://www.numerama.com.
259. S. S. Arora, "Call for Contributions to Help Identify Europe's Most Critical Open-Source Software", FOSSEPS, European Commission, March 23, 2022, available at: https://joinup.ec.europa.eu.
260. ANSSI and CEA, "L'ANSSI et le CEA renforcent leur collaboration en cybersécurité", *op. cit.*
261. European 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", COM(2022) 454 final, September 15, 2022, art. 37 and art. 10.

The EU's Next Generation Internet (NGI) initiative, led by DG CONNECT, is a funding vehicle. It supports open source projects that contribute to the development of a "human-centered Internet", i.e. contributing to offer users alternatives on all elements of the software stack, respecting European legislation (RGPD), and promoting trust, inclusiveness and multilingualism.[262] While it once supported projects from companies developing proprietary products or solutions, the NGI now only funds open source projects. The NGI's starting point is the observation that European research funding systems, such as the Horizon program, are little compatible with the dynamics of the digital world and open source: they are often large-scale funding programs requiring multi-country teams, whereas open source projects are usually produced and maintained by individuals or small teams.[263] The €82 million NGI fund for the period 2018-2020 were allocated to about 800 projects, 80% of which are led by individuals, and 90% of which are based in Europe (also some projects in the UK, U.S. and Asia). €103 million are planned for the 2021-2024 period.

Some member states are also mobilizing to financially support the open source ecosystem. Germany launched in October 2022 the Sovereign Tech Fund.[264] The project is ambitious. In particular, it seeks to tackle the often neglected issues of maintenance and scaling of open source programs, which are becoming structural components of the software infrastructure.[265] The main novelty is the creation of a fund for individuals, SMEs, collective projects, or communities developing fundamental technologies in different priority areas: Internet protocols, security certificates, DNS servers and operating systems, compilers, knowledge bases, server management... The budget forecast for this project is €10 million per year.

Towards a More Strategic Approach?

As mentioned, the EU countries are among the best students in terms of opening up public data, and a European political vision of open source exists, rooted in the issues of sovereignty and maintaining an open and collaborative Internet. However, the level of knowledge of decision-makers, of politicization and of strategic thinking around the issue of software, and open source in particular, remains low, and in any case lower than in the United States and China.[266]

262. Interview, DG CONNECT, September 2022.
263. *Ibid.*
264. Open Knowledge Foundation Deutschland, "Sovereign Tech Fund: Feasibility Study to Examine a Funding Program for Open Digital Base Technologies as the Foundation for Innovation and Digital Sovereignty", October 2021, available at: https://sovereigntechfund.de.
265. *Ibid*, p. 4.
266. European Working Team on Digital Commons, "Towards a Sovereign Digital Infrastructure", *op. cit.* interview, DG CONNECT, September 2022; interview, Project officer to the Ambassador for Digital Affairs, July 18, 2022.

Now, since the beginning of 2022, there has been renewed political attention to the subject. At the level of the European Commission, involvement is growing; it is an incremental process that is moving forward "step by step".[267] This political awareness is attributable in particular to Log4Shell and to the action of France, which held the presidency of the EU Council in the first half of 2022. In February, France declared that it wanted to set up a European strategy for the digital commons, and launched an invitation to member states to form a working group on the subject. Nineteen member states responded positively,[268] leading to a series of eight meetings over four months. Some of the participating member states indicated that they had never dealt with this topic before, so the French invitation helped to create a "spark", to put the topic on the table and, for these governments, to consider including open source and the commons in their national digital strategies.[269]

The taskforce published a report in June 2022 and promoted a common approach to the digital commons. In particular, it suggest engaging policymakers more directly in a broader and more strategic approach to OSS:

> "It is striking to notice that the vast majority of the ongoing initiatives at all levels focus on encouraging and supporting the development, use and purchasing of FLOSS and digital commons in public administration [...] However, a strategy for digital commons cannot be designed through public service centered lenses".[270]

The authors thus call for proactively identifying emerging technologies requiring development in terms of language protocol and software, and directing funds to certain key areas or infrastructures – beyond e-government tools.[271] Examples of strategic software issues for Europe include operating systems, search engines, social networks, and microprocessors.[272] Finally, the report notes a lack of coordination between European open source initiatives, which are mostly developed at the national level.

267. V. Daffey, "Open Source: Driving the European Digital Decade", Open Forum Europe, Conférence, Brno (Czeck Republic), September 16, 2022, available at: www.youtube.com (minute 42').
268 Germany, Belgium, Croatia, Czeck Republic, Denmark, Spain, Estonia, Finland, France, Ireland, Italy, Latvia, Luxembourg, Malta, Netherlands, Poland, Portugal, Slovenia, Sweden.
The Commission and the EEAS supported the initiative, without being directly involved in the drafting of the report.
269. Interview, Project officer to the Ambassador for Digital Affairs, July 18, 2022.
270. European Working Team on Digital Commons, "Towards a Sovereign Digital Infrastructure", *op. cit.*, p. 25-26.
271. *Ibid.*
272. Interview, DG CONNECT, September 2022.

Faced with these observations, the report proposes some courses of action:

- Creating a one-stop shop to collect and centralize information on national and European open source funding programs, and facilitating the application process for developers and maintainers;
- Launching multi-country calls for projects for European open source projects in strategic open source components;
- Establishing a European Foundation for the Digital Commons. This autonomous structure could emerge on the basis of a one-stop shop, and could be governed collegially by "commons" and open source actors, member states and the EU. Such a structure would "ensure independence from organizations ruled by foreign laws and to promote the development of digital innovations based on European ethical values".[273] Alternatively, the structure could take the form of a public-private partnership, such as the one that exists in photonics. The structure would aim to animate the European open source ecosystem, organize financial support for the commons, make policy recommendations, lead efforts to secure and audit open source components, and provide a platform for open source code repositories.

The establishment of a new European structure is not the most likely outcome at this stage. But it is noteworthy that the French Presidency of the Council of the EU has given way to the Czech Presidency, which in the second half of 2022, has continued the reflection and awareness-raising efforts of European decision-makers on open source. This greater political attention and more strategic vision of open source, as well as the relocation of foundations and the opening of Linux Europe, indicate that the influence of the EU and its member states on the global open source ecosystem will continue to grow, and that the European vision deserves to be promoted.

273. European Working Team on Digital Commons, "Towards a Sovereign Digital Infrastructure", *op. cit.*, p. 29.

Conclusion: Will Open Source Fall Victim to Geopolitics?

Open source plays a central role in software development, both in parallel with the proprietary model, and increasingly intertwined with it. It has become a major factor for digital companies' success. Beyond that, open source is the foundation of critical software bricks and of Internet languages and protocols, and it plays a role in the development of emerging technologies. However, open source can be a victim of its own success due to a lack of resources for maintenance, as illustrated by recent cases of software vulnerabilities with global consequences. At the same time, private companies are investing ever more money and human resources in the development and maintenance of the ecosystem. This support is critical to mitigate the risks associated with the lack of maintenance of certain components. However, we have seen that this involvement is not without risk for the open source ecosystem, which is increasingly shaped by the private interests of the Big Tech.

Two dynamics thus coexist: one in which open source is structurally fragile despite its strategic importance, both economically and in terms of security, and suffers from a lack of resources, particularly for the maintenance of components; and the other in which it is the object of investment and capture, or even misappropriation, by large technology companies. These two trends create frustrations in the open source ecosystem and may lead to a desire to pursue an ideal that would autonomize open source communities from private sector actors, even though the intertwining of the models is now a given. The question remains how to ensure that private sector interests do not hijack the principles of open source and, by extension, alter the added value of the model.

But there is a third ongoing dynamic: states have understood the critical importance of open source, and are increasingly treating it as a strategic issue. We have examined how the United States, China, and the European Union and its member states have taken up the subject. The motivations of states to invest in open source can stem from various types of objectives:

1) to access trusted technological solutions in the context of the digitization of public administration and services;

2) to ensure cybersecurity by investing in the durability of the ecosystem and the maintenance of open source components useful to the state and more broadly to the global digital architecture;

3) to develop a local software industry and reduce dependence on foreign proprietary software;

4) to preserve a certain idea of an open, public, common and collaborative digital space.

However, it is not easy to develop public policy tools to deal with an object such as open source.[274] One difficulty is that governments can do little at the level of open source communities, their governance or their legal structuring, as these are functions performed by foundations. They also have limited means of action regarding the use of open source by private companies, or regarding the misuse of open source principles and free licenses. The state's action is therefore focused on the security and maintenance of components. In the United States and Europe, parallel initiatives are emerging to strengthen the involvement of public authorities in the inventory of critical open source components, in the examination of security risks, and in the financing and maintenance of these components, in a public-private approach.

While the interest of governments in this strategic issue is commendable, one may wonder about the effects that this greater involvement of governments will have on the open source ecosystem, where the state was, until recently, only a consumer and contributor among many others. On the one hand, the coherence between these different initiatives at the international level must be considered, so as not to duplicate efforts or create contradictory standards, and to avoid security drifts. The interest in having a repository that archives and secures the most used source codes is shared by all. The tools developed by public authorities to improve software security, such as the American Software Bills of Materials and their European equivalent, could also be harmonized.[275] A coordination effort must therefore be made.

Another dynamic that is far more worrying concerns the intrusion of geopolitics into the issues of the global open source ecosystem. In the United States, national security actors identify risks of interference in open source codes via contributors working for foreign governments. It has also been mentioned that developers from countries under U.S. sanctions can be suspended from the GitHub platform, as was the case with Iran and now Russia. In addition, some see open source as a risk that U.S. adversaries, primarily China, could use it to acquire U.S. technology and circumvent sanctions. In China, government control over open source communities is increasing, as Beijing attempts to apply techno-nationalist principles to open source.

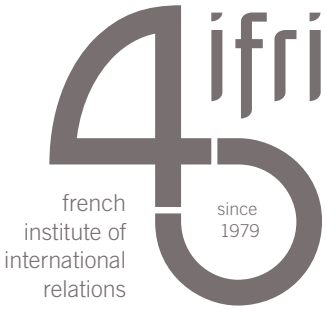
274. This is also the view of the American think tank Atlantic Council's open source initiative, launched in July 2022. They believe that the principles responsible for the success of open source – low barriers to entry, transparency and collaboration – are difficult to navigate using traditional policy tools. Atlantic Council, "Atlantic Council Launches Open-Source Software Security Effort", Press communication, July 18, 2022.

275. C. Carey, "EU's Efforts to Secure Open Source Software", Open Source Summit Europe 2022, Dublin, September 14, 2022.

All of these trends risk leading to both fragmentation and centralization of open source communities nationally, which would be harmful to an ecosystem that is currently decentralized and relatively horizontal. The European discourse, on the other hand, seeks to combine the ambitions of digital sovereignty and the preservation of the digital commons. If its room for maneuver has been rather small until now, insofar as most of the major open source players are American, Europe benefits from this globalized ecosystem, and its open and less security-driven approach than in the United States makes it an increasingly important player in the global ecosystem. This has been demonstrated by the relocation of Eclipse to Belgium, RISC-V to Switzerland, and the creation of the "Europe" branch of the Linux Foundation.

Finally, the European vision must be articulated with the EU's diplomatic positions. There are certainly avenues for cooperation with the United States and other countries in areas where both the priorities of states and the interests of open source communities converge, such as the inventory and maintenance of critical open source components. Conversely, while China is sometimes referred to as a possible, de facto "ally" of the EU in certain domains of open source like CPUs[276]. While China shares Europe's objective of greater autonomy in the face of the proprietary solutions of Big Tech, the turn taken by the Chinese government cannot make it a political ally to the European ambition. However, there is a real opportunity for Europe to reach out to partners – not only the United States but also India or Brazil, which could adhere to and help promote a vision that aims at preserving the digital commons and an Internet that is open, interoperable, respectful of freedoms and human-centered.

276. Interview, DG CONNECT, September 2022.



27 rue de la Procession 75740 Paris cedex 15 – France

Ifri.org