DIGITAL RESILIENCE FORUM

2025 REPORT

CONTENT

Impressum

Authors:
Georg Link, Jamie Ayala, & Daniel Izquierdo

Publisher: Bitergium SL ("Bitergia")

Legal Representative:
Santiago Dueñas, Administrator

Contact: info@bitergia.com

https://doi.org/10.82069/DRF.202511

Registered Address:
Av Gregorio Peces Barba 1
28919 Leganés, Madrid, SPAIN

Commercial Registry Data: Entered in the Register of Companies of Madrid, Volume 30.234, Section 8, Page 180, Sheet M-544180, entry 1

Tax Identification Code (CIF):
ESB86533882

Welcome

By Daniel Izquierdo Cortázar, CEO, Bitergia

Welcome to this first edition of the Digital Resilience Forum. A central place for discussion on how to make our software-driven societies, public and private services, and digital infrastructure more sustainable over time.

Resiliency is a term that embraces different layers in our society, from politics and policymakers to industry and academics. And this resiliency relies nowadays mainly on software. However, software is not part of today's society discussions. In this polarized world, where politics are noisy and barriers are growing across countries, software is still one of the few places where collaboration is reinforced and makes sense.

Today's software building blocks are mainly open source related. Studies claim that any new modern application contains up to 90% of existing open source technology. This is indeed key for innovation, fast development, and any new company will choose open source by default.

This is positioning open source in a very interesting way, and this is politics. Open source is now a strategic asset, but given the nature of its development as geographically distributed, this is *owned* by everyone and by no one. And this opens great opportunities to make our societies and the services we rely on more independent from third parties, while at the same time, preserving the pace of technology innovation.

And yes, open source has its own gravity in this forum as this is literally everywhere, but open source does not have all the answers to our questions. However, the transparency of open source allows decision makers to consistently audit the code of what they are consuming and who is producing this code.

> *Technological independence or digital sovereignty are terms that mean nothing without fully learning and understanding the risk of our software dependencies.*

There is a term that we discussed during the Forum and this is SBOM - Software Bill of Materials. This is the first step in understanding what our dependencies are; most of them are open source. And this transparency should come from our suppliers and providers, and be reinforced and required from those paying for the service, including public administrations or us as citizens.

Technological independence or digital sovereignty are terms that mean nothing without fully learning and understanding the risk of our software dependencies. And this is something bigger than simply choosing a different provider. This is about auditing who is producing the code we rely on including geographical regions or corporations behind this, how this is produced, including software engineering and security practices, and finally its level of maintenance and potential sustainability over time.

The Digital Resilience Forum is a place to learn what others are doing, and apply those lessons learned to our context. This conference is designed with the purpose in mind of having time for open discussions, hands-on through the workshops, and open in our minds new lines of thought the keynote presentations.

I really hope that this conference is the starting point to have software as a first level citizen in all industries and public administrations.

Global Challenges Require Global Collaboration

By Omar Mohsine, OSS Coordinator, United Nations

Since its founding, the United Nations has been built on a simple yet profound belief: *global challenges require global collaboration.*

The Charter of the United Nations recognizes that peace, prosperity, and human development cannot be achieved in isolation. No single country, institution, or organization—no matter how powerful—can solve the world's most pressing problems alone. From climate change to humanitarian crises, our progress has always depended on our ability to work together, share knowledge, and elevate collective wisdom over individual interest.

Today, this fundamental principle of collaboration extends beyond borders, cultures, and governments. It now lives and thrives in the digital world. Every day, millions of people—most of whom will never meet and may never even know each other's names—collaborate online to build software that powers our societies. This movement is known as open source. It represents one of the most extraordinary demonstrations of human cooperation in history. Contributors from every corner of the world voluntarily create, improve, and secure the digital infrastructure that our economies, our public services, and our future depend on.

The principles that underpin open source—openness, transparency, and community—are the same values that guide the United Nations. Open source is not just a technical model; it is a governance model. It proves that when we share ideas and capabilities openly, we accelerate progress and strengthen resilience. It turns users into contributors, consumers into creators, and isolated systems into interconnected ecosystems.

As the world enters an era defined by digital transformation, Member States collectively recognized that our future requires cooperation and shared rules. This commitment is now reflected in the Global Digital Compact, adopted by all governments of the world, which underscores that we cannot achieve the Sustainable Development Goals without digital technologies. And we will not build the digital foundations we need without openness, shared innovation, and collaboration.

Digital resilience is not only about having strong and secure systems—it is about empowering communities, enabling local innovation, and ensuring that the benefits of technology reach everyone. Open source gives us a pathway to do exactly that.

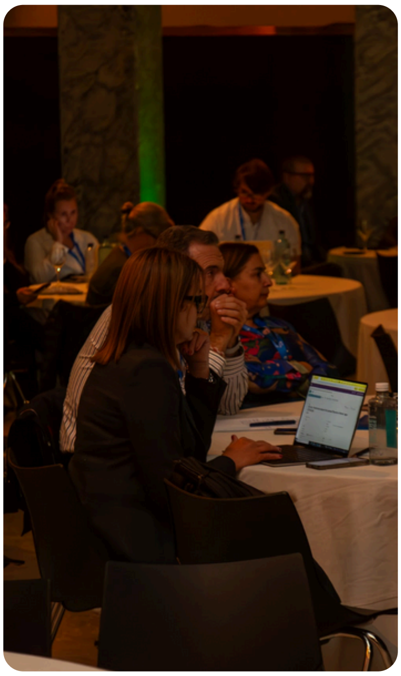
Let us seize this opportunity—not only to build digital systems that are resilient, but to build a digital future that embodies the best of who we are: a global community committed to cooperation, to shared progress, and to leaving no one behind.

Open Source not Local Source

By Amanda Brock, CEO, OpenUK

There's a profound misunderstanding across Europe around open source. I can live with people seeing what they want in this software: those on the left see it as socialist software, while libertarians believe it enables the free market through innovation and competition. In essence, open source democratises tech, and makes the results available to everyone. However, I cannot live with the misguided thinking that lies behind the concept that open source is the "cornerstone of digital sovereignty." That's a juxtaposition.

It's open source, not local source.



Today's platforms are based on open source software. Building a software stack today is impossible without open source, let alone building one that excludes technology from certain countries.

Open source requires human readable source code that is shared under a licence meeting the Open Source Definition. Anyone can use the code for any purpose, subject to applicable laws. There's no requirement that all contributions are accepted or that everyone can contribute. Successful open source projects are picky about what enters their codebase based on quality of contribution, not nationality of contributors.

Open source's international community didn't discriminate against anyone's nationality until 2024, when the Linux Foundation excluded 13 Russians from being Linux Kernel maintainers. No clear explanation was given, just a report on sanctions allowing conclusions to be drawn. Other US organisations claim this approach is not required for sanctions compliance. To enshrine the nature of open source's collaborative beliefs for the future we must push-back hard on such restrictions - to the extent legally permissible.

Over the last 30 years a few, primarily US, companies have grown to dominate the tech landscape. In the mid 90's we could not have foreseen that a handful of companies and their wealthy founders would be so influential today. Digitalisation has resulted in dependency on software to build and distribute products. With hindsight, governments would undoubtedly have taken very different approaches to the market and to its regulation.

Silicon Valley's environment enabled growth, building today's front runners that focus on "shareholder value" as the only measure of success. The capacity of these few companies to buy up innovative global start-ups before they scale locally has generated incredible value and enshrined the US as the centre of digital power with all nations except perhaps China dependent on these US companies for technology today.

Governments across the world recognise this dependence today. Those same governments have struggled to understand the tech sector, its money flows and its success transforming into dominance. Margarete Vestager, the EU'S Competition Commissioner and EU President Ursula Von Der Leyen pushed back hard on US companies, seeking to break the EU's dependency on their services for years.

Aggressive EU sovereignty demands have been unsubtle and often exclusionary. In the face of perceived anti-American behaviour evidenced by EU laws, court cases and business initiatives, it is unsurprising that the Trump administration has reacted to protect the US tech sector.

To achieve digitalisation requires open source. The massive gaps in locally available digital stacks can only be filled by open source. Collaborative, global open source outputs are freely available for this usage, but ultimately it's a form of dependency on international technology. Worse, it leads to rework and the risk of missing updates and innovation through forking global projects to become "local" projects supported in specific countries or regions. Call a project German, French or even British, but its contributors are global as are the dependencies upon which it is built.

The UK Compute Roadmap is unusual in setting a sovereignty position that is not "isolationist" and sits between multiple nations, allowing global collaboration and a pathway to openness.

Nvidia CEO Jensen Huang talks of a nation's "intelligence" to describe how technology is shaped by its language and culture. We need technology that can be localised to enable and enshrine this "intelligence." It's a great marketing strategy for Nvidia, but it happens to ring true. What really matters isn't where technology is created but the ability to localise and "access" that technology. This access alleviates the risk of dependency and geopolitics.

Why Do You Trust Software? I Don't.

By John Ellis, President & Head of Product, Codethink Ltd.

Software has become the critical infrastructure of the modern world, yet society continues to treat it as disposable. From hospitals and autonomous vehicles to financial markets and national grids, reliability has become assumed rather than engineered. The past two years, marked by the 2024 CrowdStrike outage, the 2025 Google Cloud failure, and continuing supply-chain breaches such as MOVEit and SolarWinds, exposed the limits of our current approaches to testing, certification, and assurance. Following, I argue that digital resilience will not emerge from compliance checklists but from measurable trust: transparent prov-enance, reproducible construction, and continuous accountability.

Global infrastructure now depends on code written by individuals and teams spread across thousands of organizations and open source repositories. The illusion of control persists, but the data say otherwise. In July 2024, a single defective update from CrowdStrike incapacitated more than eight million Windows systems worldwide. Flights were canceled, hospitals reverted to paper, and financial services ground to a halt, an estimated $10 billion in losses. Less than a year later, Google Cloud's Service Control outage cascaded across core internet services. None of these events were cyber-attacks; they were self-inflicted.

The lesson is brutal but clear: software failure is now a systemic risk, not an operational inconvenience.

The industry's obsession with "security" often substitutes visibility for reality. As Bruce Schneier warned two decades ago, much of what passes for protection is security theater, the appearance of safety without substance. Enterprises advertise AES-256 encryption while leaving default passwords untouched. Vendors race to add "AI-secured" badges while their build systems remain opaque and unaudited. Standards such as ISO 26262, DO-178C, and IEC 61508 are valuable, but fragmented; they create silos of compliance rather than a universal language of trust.

The result is a patchwork of certifications that impress auditors yet do little to prevent a misconfigured update from disabling an airline fleet.

Testing remains the cornerstone of software assurance, but “passing tests” does not equal “being trustworthy.” CrowdStrike’s defective driver was tested, extensively, before deployment, yet it caused major damage. Testing demonstrates conformance to expectations under known conditions; trustworthiness demands evidence of resilience under failure.

The engineering world understands this distinction. Bridges are not trusted because they are tested to hold a specific load; they are trusted because they are designed with quantified margins of failure. Software needs the same philosophy.

Between 1995 and 2025, cumulative economic damage from software incidents is estimated between $10 trillion and $19 trillion. Yet the industry lacks any consistent way to price or compare risk. Unlike finance, which built credit scoring and actuarial modeling to tame uncertainty, the digital sector continues to fly blind. “We have trillion-dollar dependencies,” Ellis argued, “and no FICO score for code.”

This absence of quantifiable trust makes it impossible for insurers, regulators, and operators to align incentives. Without metrics, risk remains invisible, and therefore unmanageable.

To address that void, Codethink and its collaborators introduced the Trustable Software Framework (TSF). TSF organizes assurance into six tenets: Provenance, Construction, Changes, Expectations, Results, and Confidence. Each tenet captures a different dimension of software trust, from where components originate to how they evolve and perform in the field.

The framework transforms abstract compliance into verifiable evidence. Its most visible output, the Trustable Score, aggregates this evidence into a dynamic 0–1000 index. Like a credit score, it updates continuously as new builds and patches emerge. The score does not guarantee perfection; it quantifies confidence.

Transparency alone is not enough; incentives must follow. In the current model, the costs of software failure are socialized while the gains of speed are privatized. Quantified trust allows for market correction. Insurers can underwrite digital systems with precision rather than guesswork. Regulators can benchmark safety across industries. Executives can justify investment in resilience through measurable risk reduction.

“Once trust becomes a number, resilience becomes a business model.”

The European Union’s Cyber Resilience Act (CRA) mandates secure development processes, traceable components, and decade-long support lifecycles. Implementing these requirements has challenged both lawyers and engineers. Frameworks such as TSF make compliance tangible: reproducible builds, SPDX manifests, and automated provenance tracking convert legal text into operational proof.

For executives, this reframes regulation from a cost center to a competitive differentiator, measurable trust translates directly into lower risk exposure and, ultimately, lower premiums.

Trustable software is no longer theoretical. Codethink’s safety-assessed Linux distribution, built under TSF principles, supports Torc Robotics’ Level-4 autonomous trucking platform. The project demonstrates that rigorous assurance and modern agile methods need not conflict. Resilience and velocity can coexist, provided evidence replaces assumption.

I closed my session at the Forum with a simple declaration: “We don’t need perfect software. We need trustable software.” The point is not pessimism but realism. Digital systems will fail; resilience is the art of failing safely. Achieving that will require cultural and structural change, shared frameworks, open metrics, and executive willingness to demand transparency from the software supply chain.

Resilience will not come from hoping the next update holds. It will come from designing every update, every dependency, every build system for the day it does not.

The Engine Room of Digital Sovereignty

By Adriana Groh, CEO, Sovereign Tech Agency

Resilience is not built in moments of calm. It takes crises for invisible systems to become visible—and for societies to remember that infrastructure is not simply what we build, but what we depend on every day. The pandemic, the war in Europe, and cascading software failures all pointed to the same structural fragility: our digital foundations were never designed to last.

When I first spoke with the German government about the need to maintain open source, I did not need to convince them with abstract arguments about innovation. I only had to show them what breaks when infrastructure is neglected. Just as bridges collapse when maintenance is deferred, digital systems decay when the code that underpins them is left to volunteers and chance. Software is infrastructure. But it is an invisible kind, one that policymakers rarely see until it fails.

This is the gap that the Sovereign Tech Agency was created to address. We treat the maintenance and provision of the open digital ecosystem as a public service, a form of *digitale Daseinsvorsorge*—a guarantee of the essential digital conditions for social and economic life. That means maintenance, not hype; collaboration, not isolation. Our programs invest directly in the components that make everything else possible: the libraries, languages, and systems that the entire digital economy quietly depends on.

Crucially, sovereignty is not isolation. It is not about replacing one commercial dependency with another, nor about drawing borders around code. Sovereignty means the self-determined use of technology: understanding how it works, how to repair it, and how to co-create it with others. It is a relational capacity that emerges from participation in shared infrastructures, not withdrawal from them.

That is why our work begins where visibility ends. We support maintainers as professionals, not hobbyists. Through the Sovereign Tech Fund, we procure maintenance contracts that reduce risk and increase stability, whether through new code or the removal of unsafe complexity. Our Resilience program focuses not only on finding vulnerabilities, but on preventing them. And through the Sovereign Tech Fellowship, we provide stable compensation to the individuals who keep critical open source infrastructure running, because infrastructure maintenance is not charity; it is an obligation, and this obligation cannot fall on one government alone.

We call for every government, not only Germany's, to build its own "engine room" for digital resilience, not as an isolated national effort, but as part of a coordinated, international effort to sustain the open commons that all modern innovation relies upon. Too often, governments equate digital policy with innovation policy. But innovation without maintenance is an illusion.

Even the world's most advanced AI models depend on decades-old open source components that are maintained by only a handful of people. Investing in their stability is a matter of industrial policy. It is the difference between a society that reacts to a crisis and one that is prepared for it. If we fail to support those maintainers, we are not risking innovation—we are risking everything built upon it. A well-maintained open source ecosystem accelerates scientific research, strengthens economic competitiveness, and supports democratic autonomy. It is the precondition for every other form of digital progress.

Resilience begins in the quiet work of maintenance, in the shared responsibility for the bridges we all cross but rarely see. Ultimately, if we want to move faster, we must take care of what allows us to move at all.

PANELS

The Path to Resiliency

Four panels with four key topics addressed and share ideas and discussions with the audience. The participants covered a diverse set of layers, including representation of governments, public administrations, the open source and open innovation ecosystems, think tanks, and private entities.

Panelists shared how they are dealing today with resiliency and its meaning for them. To later discuss the implications of technology, its quick evolution, the fragility of these ecosystems, and how to make them more open, sustainable, and accessible to everyone.

Transparency, knowledge, technology, decision-making capacity, and pragmatism were the basis of the discussions.

Maria Antonia Bravo, Programme Manager at Giga a UNICEF–ITU initiative
Juan Corro, CIO, Madr
Council
de Galicia
LET'S BUILD A STRONGER DIGITAL WORLD, TOGETHER

PANEL

Growing Resilience

International Initiatives and Lessons Learned

The panel advanced our understanding of digital resilience by defining it as the outcome of robustness and continuity. This is not to be confused with digital sovereignty, which is the strategy of control and choice.

Tanya Suarez Ph.D, CEO of BluSpecs
Gina Plat, Interim Lead for OSPO at the Ministry of the Interior and Kingdom Relations
Gar T. MacCriosta, Digital Advisor and Product Manager for Ireland's Health Service Executive
DIGITAL RESILIENCE FORUM

Panel Moderator: **Jennifer Tridgell**, International Lawyer and PhD Candidate at University of Cambridge

Panelists:

- **Tanya Suarez** Ph.D., CEO and founder of IoT Tribe
- **Gina Plat**, Interim Lead for the Open Source Program Office at the Ministry of the Interior and Kingdom Relations Netherlands
- **Gar Mac Críosta**, Health Service Executive (HSE) in Ireland

Resilience, they argued, must be built across three operational levels. First, individual resilience focuses on foundational security, such as effective password management.

Second, business resilience addresses continuity and the practice of building hardware and software stacks designed specifically to operate in the face of attacks. Finally, state resilience refers to the collective
ability of nation-states and communities to provide a sense of safety and continuity for everyday life.

The most critical challenge identified is "crippling technical legacy." This includes 50 years of aging infrastructure, exemplified by the HSE's systems, that requires deep, systemic fixes. It will not be enough to pursue minimum compliance with regulations like the EU Cyber Resilience Act (CRA). This deep-seated technical debt remains the primary obstacle to modernization. To overcome this, the panel stressed that governments must intentionally create market pull for high-quality, resilient solutions, moving beyond legacy procurement habits that favor large vendors.

Progress hinges on fostering global collaboration and strategic funding. Initiatives like the Netherlands' open unless policy and the European Digital Infrastructure Consortium (EDIC) are key to establishing this market pull. These structures need better data and analysis of open source projects and communities to inform procurement decisions. Critically, such thoughtful investment choices are necessary because open source's lack of restrictions can pose a severe risk to critical infrastructure without intentional, domain-specific risk management. By funding these efforts, governments prove they can move beyond relying on fragile systems to actually designing in long-term resilience.

Sustainable Innovation Through Open Ecosystems

Governance, Talent, and Collaboration

This panel framed digital resilience is a strategic outcome dependent on verifiable collaboration, transparency, and data-driven governance of the entire open ecosystem.

Panel Moderator: **Emily Omier**, OSS Consultant, OSS Founders Summit co-founder and Host of Business OSS Podcast

Panelists:

- **Alberto P. Martí**, VP of Open Source Innovation, OpenNebula Systems
- **Ana Jiménez Santamaría**, Senior Project Manager, the Linux Foundation
- **Clare Dillon**, InnerSource & Open Source Advocate, Open Ireland Network
- **Melanie Wollnik**, facilitator at OpenRail Association

The discussion established that merely using open source software does not guarantee collaboration or transparency. Such unchecked assumptions expose companies and governments to unmanaged risk, undermining the very digital resilience they seek.

While innovation and resilience depend on diverse collaboration, this activity does not happen organically or effectively without support.

To build truly resilient and trustworthy systems, organizations require tools to move beyond assumptions and objectively quantify engagement across all contributors.

Strong governance is critical in complex and high-stakes domains like legacy industries where safety is critical, or in AI/ML, where governance must span code, models, and data. Monitoring key community metrics is necessary to ensure projects meet established standards and support sustainable innovation.

The panel emphasized that a project's commitment to community engagement is the best indicator of its long-term viability. Skills for working in open source cannot be taken for granted but need to be taught, just like the culture of open source. With such a foundation in place, for example by working with an open source foundation, innovation can be unlocked. In Europe, the panelists see such innovation often rooted in a focus on social aspects and the desire to make technology useful for people while considering potential harm up front.

PANEL

Workforce 2025

Digital Skills, Institutions, and the Path to Resilience

The panel discussed the failure to align talent pipelines with industry needs. Achieving digital resilience is difficult in the face of an unquantified gap between the lack of advanced digital skills and the actual demands of the market.

Moderator: Elzbieta Godlewska, Global Partnership, Linux Professional Institute
Maria Antonia Bravo , Programme Manager at Giga a UNICEF–ITU initiative
Juan Corro, CIO, Madrid City Council
Carlos Vázquez, Director, Centro de Novas Tecnoloxías de Galicia (CNTG)
Virgilio D. Deputy Director, Entrepreneurship and Innovation Support Service, C3NIA

Panel Moderator: **Elzbieta Godlewska**, Global Partnership, Linux Professional Institute

Panelists:

- **Juan Corro**, Madrid City Council CIO
- **Carlos Vázquez,** Director do Centro de Novas Tecnoloxías de Galicia (CNTG), Consellería de Emprego, Comercio e Emigración Xunta de Galicia
- **Maria Antonia Bravo**, Programme Manager at Giga a UNICEF–ITU initiative
- **Virgilio Díaz**, Deputy Director, Entrepreneurship and Innovation Support Service at C3NIA Science Park, Carlos III University of Madrid

A foundational shift is required in education to address this, beginning with the universal integration of computational thinking as a core competency. This training is essential not just for using new tools, but for equipping the future workforce to effectively govern and manage AI-driven systems.

Furthermore, the resilient professional must be holistically developed, meaning that technical skills must be paired with humanities and soft skills, such as cross-team collaboration, communication, and problem-solving. This combination ensures that technical experts can successfully deploy and manage solutions within societal contexts.

The panel highlighted that effective talent resilience depends on strong training strategies that align directly with market realities. This is achieved through programs that are co-created with industry and emphasize "learning by doing" with real projects, validated by sought-after vendor certifications. Open source software offers such a learning environment. This model speeds up adaptation and ensures higher immediate employability.

Ultimately, the understanding of digital resilience is informed by the conclusion that it is partially a "question of mind," underscoring the necessity of providing all personnel with the psychological and intellectual tools to navigate and manage constant technological change and uncertainty.

Digital Resilience in Practice

Securing the Digital Supply Chain

The panel deepened our understanding of digital resilience by moving the conversation to focus on traceability, data integrity, and strategic foresight.

Panel Moderator: **Juan Rico**, Senior Program Manager at Eclipse Foundation Europe

Panelists:

- **Stefano Zacchiroli**, Co-founder and CSO (Chief Scientific Officer) of Software Heritage
- **Philippe Ombredanne**, Lead Maintainer of AboutCode
- **Darío García de Viedma**, Fellow at the Elcano Royal Institute in the fields of technology and digital policy
- **Georg Link**, Open Source Strategist and Director of Sales at Bitergia.

A critical insight was that the industry is currently "flying blind" due to a lack of transparency in the software supply chain. Organizations struggle to produce a complete and accurate inventory of all open source components in use, which is the foundational data needed for judging the resilience of a system. The panelists emphasized that this data deficit is made worse by often-unreliable scanning tools and siloed, duplicated scanning because metadata is not standardized or shared.

The discussion firmly established that achieving resilience requires a reframing. We must prioritize resilience and common societal goals in technology design, rather than perpetually mitigating harm after the fact.

Resilience relies on adopting standards like SBOMs (SPDX, CycloneDX) and cryptographic identifiers (SWID, PURL) to achieve end-to-end traceability. Furthermore, utilizing public archives (like Software Heritage) is a necessary fallback to ensure the permanent availability of source code, protecting against sudden platform failures or geopolitical blocks.

Open source's critical status means it is now a tool for geopolitical competition, risking the fragmentation of its universal nature. This trend introduces new vulnerabilities that can only be countered by strong, collaborative, and well-governed open source communities.

In short, digital resilience is not a feature you buy; it's a discipline you practice through better data, verifiable standards, and active community engagement. The challenge is not external—it's organizational and structural, demanding a more transparent, standardized, and archivally secure approach to how all software is built.

WORKSHOPS

Practical Application

Four workshops, stressing the practical approach and more time for interactions, were on stage.
From introductory topics for those willing to learn the basics and discuss with experts in the field, to those covering technical details.
These covered essential topics for our digital lives as our digital identity and how to implement this, the process to start effectively managing technology, and especially open source and the role of the program offices for this, the impact of public funding in technology and the role of the Sovereign Tech Agency, to finally discuss unexpected events and how to have disaster recovery policies and actions in place.

WORKSHOP

Kick-Starting Your OSPO

A practical approach

The workshop focused on why companies need a special team called an Open Source Program Office (OSPO). The OSPO acts as the central control point, or "center of gravity," for managing a company's use of open source software and making sure its digital operations can last a long time.

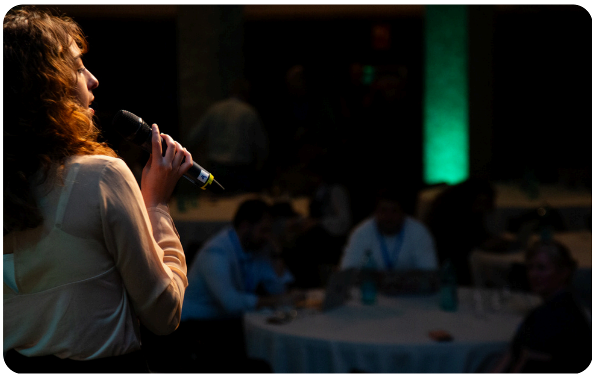
Workshop Facilitators:

- **Ana Jiménez Santamaría**, Senior Project Manager, the Linux Foundation
- **Dawn Foster**, Open Source Strategy Consultant | Director of Data Science, CHAOSS Project

The workshop showed that the OSPO has to connect with everyone: upward (getting approval and money from top leaders), downward (managing its own tasks), sideways (working with other departments), and outward (dealing with outside open source communities). Getting support from top leaders is the most important step for getting the resources needed. The OSPO's main jobs include lowering risks, improving security, talking with the community, and building a strong open source culture.

The workshop used a guide called the OSPO Book from the TODO Group. The session mixed short talks about how an OSPO is set up with three hands-on group activities. Attendees worked to determine their company's goals for open source, decide which tasks to undertake first, and assess their current position on the "Open Source Journey" (i.e., whether they are simply using open source or actively contributing to its development). This practical work made participants deal with a key idea: a universal OSPO plan won't work everywhere; it must be adjusted for each company's unique culture—"My OSPO is not your OSPO."

A takeaway was the problem of not having enough resources; for example, many OSPOs don't have enough staff. It's also hard to get everyone inside the company to agree on what the OSPO should do. A big part of the workshop focused on making security better by making it a shared responsibility and building security checks into the developers' daily work, rather than fixing problems later. Most importantly, the discussion highlighted that OSPOs must link the simple benefit of using open source with the necessity of contributing to it. They need to push for employees to get recognized for their contributions to keep the essential maintenance work going.



Building Resilient Digital Trust

Infrastructure with First Person Credentials

The workshop addressed digital resilience by proposing a decentralized solution to fortify the open source supply chain against systemic threats like the XZ attack and unverified AI contributors.

Workshop Facilitator:

- **Drummond Reed**, Founder, First Person Project

The central tenet of the First Person Project is to provide verifiable Proof of Personhood using a new trust infrastructure. This infrastructure aims to make open source more resilient by cryptographically assuring that code changes originate from unique, authenticated human developers, thereby mitigating Sybil attacks and ensuring accountability.

The session was delivered as an in-depth architectural overview, complete with analogies to the TCP/IP stack and the PGP Web of Trust. The speaker, Drummond Reed, detailed the Trust over IP four-layer model, which includes a trust-spanning protocol (TSP) and separates cryptographic verification (DIDs) from human trust (Verifiable Credentials).

Key concepts, such as the Trust Triangle, Governance Diamond, and the role of digital wallets, were introduced. The presentation concluded with a Q&A segment focusing on implementation and adoption pathways, including the immediate pilot program with the Linux Kernel Project.

Participants gained insights into building a Decentralized Trust Graph using two distinct credentials: the unlinkable Personhood Credential, which ensures uniqueness within an ecosystem, and the Verifiable Relationship Credential (VRC), which establishes cryptographically strong peer-to-peer trust. They learned how this model, leveraging Zero-Knowledge Proofs (ZKP) for unlinkability and using Personas to control identity context, offers a robust, privacy-preserving alternative to centralized biometric databases. This infrastructure paves the way for secure open source contribution and scalable transactions involving personal AI agents.

DIGITAL RESILIENCE FORUM

WORKSHOP

Disaster Recovery

Hands on Workshops, led by BBC

The workshop centered on enhancing digital resilience through robust Disaster Recovery strategies, moving beyond standard failure responses to address catastrophic losses of core infrastructure.

Workshop Facilitator:

- **Tom Sadler**, Principal Software Engineer at the BBC and Member of the InnerSource Commons Foundation

The session specifically focused on maintaining service continuity and availability even when major upstream dependencies (like AWS accounts or GitHub) become entirely inaccessible, requiring deep systemic preparation.

The session format was a hands-on working group exercise led by Tom Sadler. After an introductory overview of the BBC's existing resilience mitigations (e.g., caching fallbacks, multi-CDN delivery, simulated disaster scenarios), the group was split into two teams.

One group focused on Software Components and Infrastructure (the "moving parts"), and the other focused on Service Features and Functionality (defining the minimum viable service). The exercise involved first sketching out a hypothetical system architecture and then, for Part Two, brainstorming technical and process-based mitigations to prevent total system failure or ensure rapid recovery.

Key insights learned centered on the need for decentralized and non-IP alternatives as extreme fallbacks, such as relying on traditional broadcast signals (peer-to-peer/over-the-air) when IP-based streaming fails. The groups identified that typical complex, tightly-coupled architectures are often single points of failure, where the loss of one component (like source control or a cloud provider) could cascade into a complete service outage. Therefore, the core takeaway was that we need to have fully tested infrastructure-as-code and external backups for critical resources, along with defining clear, low-fidelity fallback service tiers to provide users with a functional minimum service during any catastrophic event.

DIGITAL RESILIENCE FORUM

WORKSHOP

The Impact of Public Funding in Technology

A global open infrastructure negotiation role playing game

The workshop was an interactive role-playing negotiation game designed to explore the systemic fragility of the open source ecosystem and the collective responsibility required for its survival.

Workshop Facilitator:

- **Paloma Oliveira**, Technologist at Sovereign Tech Agency

The session's primary goal was to help participants internalize the complexity of funding and maintenance crises in critical digital infrastructure.
The format was a role-playing game called "The Commoning Crisis," led by Paloma Oliveira. Participants were assigned one of five stakeholder roles—Developer, Government, Industry, Researcher, or Civil Society—plus a facilitator role (the Sovereign Tech Agency Agent). Each role was given specific resources (money, influence, trust, personal capacity) and conflicting objectives.

The core of the workshop involved negotiating solutions to two dramatic, hypothetical, time-bound crises ("Critical Vulnerability" and "Funding Freeze") within small groups, forcing players to prioritize survival and trade-offs.

Key insights emerged from the solutions proposed and the ensuing discussion: First, the current open source model has an existential dependency on individual, often unpaid, maintainers, highlighting the need for structured, sustainable funding to prevent burnout and mitigate single points of failure. Second, successful solutions required cross-sector collaboration, where government funds, industry resources, and community capacity (like academia or fellow contributors) were combined to provide support (e.g., funding a fellowship or emergency retainer). The exercise underscored that digital sovereignty and service continuity are not purely technical problems, but are inherently political and economic challenges that require coordinated public and private investment, as well as a shared understanding of technology's invisible, yet essential, nature.

THE FORUM IN NUMBERS

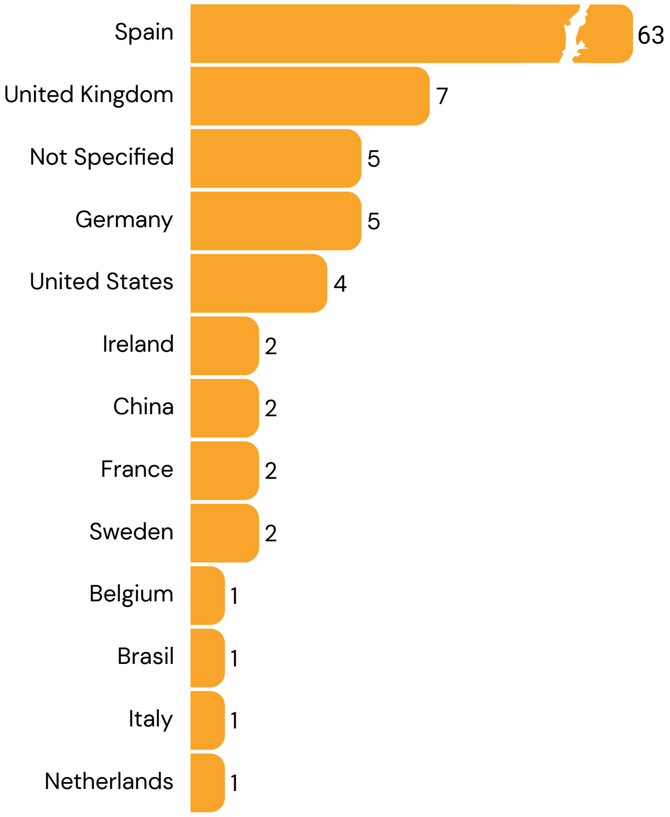
The Forum brought together many different industries, sectors, and organizations, representing a diverse set of views.

The day left much time for networking and exchanging ideas, both one-on-one and in group settings. The engagement was phenomenal and extended also into the digital realm of LinkedIn.

This section breaks down the event's reach, offering a clear statistical look at who participated, where they came from, and what they represented, providing a quantifiable measure of the community's diversity and active involvement.

Attendees

Demographics

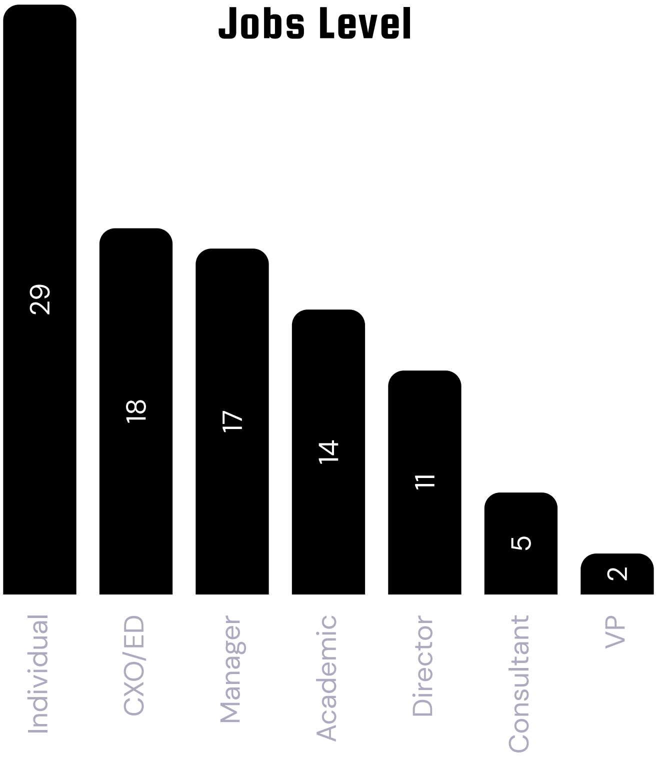


168 Registrations

96 Attendees

Industry	Attendees
Open Source - Technology	29
Education – Research & Higher Education	17
Technology	10
Government – Public Administration	8
Consulting	5
Not Specified	5
Non-profit Organization	4
Research & Policy / Innovation & Data Science	3
International Policy and Development	3
Fintech	3
Telecommunications	2
Legal Services – Corporate & Technology Law	2
IT Services	2
Healthcare Service	4
Insurance	1
Aviation & Airlines	1

Jobs Level



Digital Impact

Website Reach

6,905

Views

2,974

Visitors

LinkedIn Reach

594

Page Views

272

Unique Followers

23,811

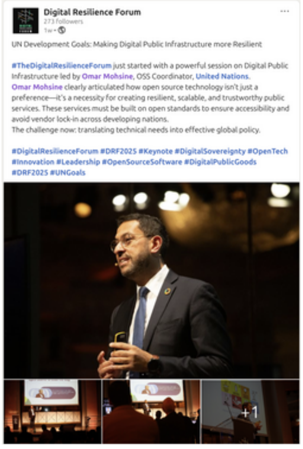
Post Impressions

991

Engagements

(Reposts, Likes, Clicks)

MOST VIEWED POSTS

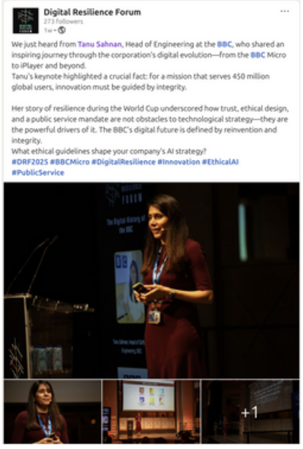


Digital Resilience Forum
273 followers
1w •

UN Development Goals: Making Digital Public Infrastructure more Resilient

#TheDigitalResilienceForum just started with a powerful session on Digital Public Infrastructure led by Omar Mohsine, OSS Coordinator, United Nations.
Omar Mohsine clearly articulated how open source technology isn't just a preference—it's a necessity for creating resilient, scalable, and trustworthy public services. These services must be built on open standards to ensure accessibility and avoid vendor lock-in across developing nations.
The challenge now: translating technical needs into effective global policy.

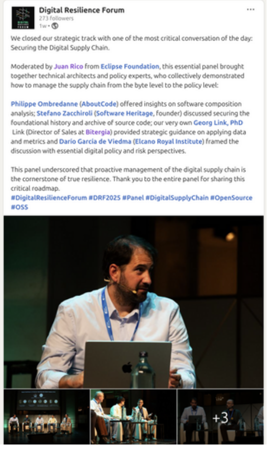
#DigitalResilienceForum #DRF2025 #Keynote #DigitalSovereignty #OpenTech #Innovation #Leadership #OpenSourceSoftware #DigitalPublicGoods #DRF2025 #UNGoals



Digital Resilience Forum
273 followers
1w •

We just heard from Tanu Sahnan, Head of Engineering at the BBC, who shared an inspiring journey through the corporation's digital evolution—from the BBC Micro to iPlayer and beyond.
Tanu's keynote highlighted a crucial fact: for a mission that serves 450 million global users, innovation must be guided by integrity.

Her story of resilience during the World Cup underscored how trust, ethical design, and a public service mandate are not obstacles to technological strategy—they are the powerful drivers of it. The BBC's digital future is defined by reinvention and integrity.
What ethical guidelines shape your company's AI strategy?
#DRF2025 #BBCMicro #DigitalResilience #Innovation #EthicalAI #PublicService



Digital Resilience Forum
273 followers
1w •

We closed our strategic track with one of the most critical conversation of the day: Securing the Digital Supply Chain.

Moderated by Juan Rico from Eclipse Foundation, this essential panel brought together technical architects and policy experts, who collectively demonstrated how to manage the supply chain from the byte level to the policy level:

Philippe Ombredanne (AboutCode) offered insights on software composition analysis; Stefano Zacchiroli (Software Heritage, founder) discussed securing the foundational history and archive of source code; our very own Georg Link, PhD Link (Director of Sales at Bitergia) provided strategic guidance on applying data and metrics and Dario Garcia de Viedma (Elcano Royal Institute) framed the discussion with essential digital policy and risk perspectives.

This panel underscored that proactive management of the digital supply chain is the cornerstone of true resilience. Thank you to the entire panel for sharing this critical roadmap.
#DigitalResilienceForum #DRF2025 #Panel #DigitalSupplyChain #OpenSource #OSS

Friends of the Forum

We are grateful for the many friends from across academia, industry, and governments who supported the organization of the Digital Resilience Forum. Their enthusiasm for the topic and encouragement were the fuel we needed on the road of creating this event.

AboutCode

CEI-Sphere part of EUCloudEdgeIoT.eu

CHAOSS

Drupal™ ASSOCIATION

ECLIPSE® FOUNDATION

Linux Professional Institute

ofe OpenForum Europe

Open Ireland Network

open logistics foundation

Open Nebula

OPENRAIL ASSOCIATION

OPEN SOURCE CONFERENCE 2025 LUXEMBOURG

Open:UK

OSS COMPASS

OSPOlogy

TODO

Sovereign Tech Agency

uc3m | C3N-IA

Sponsors

The event was only possible because of our awesome sponsors! A huge Thank You!

PLATINUM SPONSOR

Bitergia

Gold Sponsors

Linux
Professional
Institute

Red Hat

Silver Sponsors

SCANOSS

Open
Nebula

Bronze Sponsors

across LEGAL

AboutCode

Open
Regulatory
Compliance

Impressions

"We are all working together to make sure that the software we all depend upon is going to last and be trustworthy." - Clare Dillon

“We don’t need perfect software. We need trustable software.” John Ellis

DIGITAL RESILIENCE FORUM

LET'S BUILD RESILIENCE TOGETHER

Reach out to discuss how Bitergia can help your organization by providing transparency and strong insights into your open source developments, community health, and key performance factors. This allows you to properly manage risk and thus support digital resilience.

✉ info@bitergia.com

🌐 bitergia.com

in Bitergia

▶ Youtube Playlist