nc3.lu
National Cybersecurity Competence Center
LUXEMBOURG

2026 LUXEMBOURG GRC SUMMIT
powered by NC3

TO WHAT EXTENT IS OPEN SOURCE CRITICAL FOR ACHIEVING CYBERSECURITY RESILIENCE AND DIGITAL STRATEGIC AUTONOMY IN THE EU?

OUTCOME PAPER

Perspectives on building a trusted and sustainable open-source ecosystem to support Europe's cybersecurity resilience and strategic autonomy, drawing on insights from the Luxembourg GRC Summit 2026 forum session on open source.

Table of contents

3	Summary
4	Open Source at the Core of the Digital Ecosystem
4	Open Source, Strategic Autonomy and Capability
5	Making Open Source Sustainable, Trusted and Usable
9	When Automation Targets Open Collaboration
11	Key Takeaways
12	Recommendations and Action Points



TO WHAT EXTENT IS OPEN SOURCE CRITICAL FOR ACHIEVING CYBERSECURITY RESILIENCE AND DIGITAL STRATEGIC AUTONOMY IN THE EU?

Summary

This outcome paper summarises the discussions that took place during the forum "To what extent is open source critical for achieving cybersecurity resilience and digital strategic autonomy in the European Union (EU)?", held as part of the 2nd edition of the Luxembourg GRC Summit on 3rd and 4th June 2026. The Summit brought together Cybersecurity Governance, Risk and Compliance (GRC) professionals, practitioners and decision-makers to exchange knowledge, examine emerging threats, and explore evolving practices in the field.

This forum drew on perspectives from incident response, academia, internet infrastructure and non-profit organisations, alongside cybersecurity practitioners from Luxembourg and abroad. The discussions approached open source as a strategic component of the digital ecosystem, supporting cybersecurity capabilities, control over critical technologies, adaptability and European strategic autonomy.

Participants also examined the conditions needed to make open source sustainable, trusted and usable, including funding, long-term support for its communities and vendors, and trust-building without unnecessary barriers. Discussions also addressed the complementary role of open standards and the challenge that automation poses to open collaboration.

Open Source at the Core of the Digital Ecosystem

01

Open source is already deeply embedded in modern digital infrastructure and end devices. Participants noted that more than 90% of software contains open-source components, often without organisations being fully aware of the extent of its presence. Open source is therefore not a marginal alternative to proprietary software, but part of the technological foundation on which many public and private organisations already rely and are building their security and services.

Internet infrastructure was used to illustrate how important this dependency has become. Autonomous systems, the Domain Name System (DNS) infrastructure and technologies such as Domain Name System Security Extensions (DNSSEC) rely on software that operators need to understand, modify, inspect and control. Using open-source components gives infrastructure operators greater visibility into how these systems function and allows them to respond more autonomously and quickly when incidents occur. Participants noted that this underlying infrastructure often remains invisible to end users, even though open source supports much of what's commonly perceived as "just the internet".

The role of open source is also particularly visible in the cybersecurity field. The threat intelligence platform MISP was cited as one successful example of an open-source project that contributes significantly to the cybersecurity ecosystem in Luxembourg and abroad. These two examples illustrate how deeply embedded open source is in our digital infrastructures, and highlight the need to consider it as a critical part of our capabilities.

Open Source, Strategic Autonomy and Capability

02

Open source was presented not only as a way to access software without paying licence fees, but also as a means of building and retaining technical capability within the organisation. While buying an off-the-shelf proprietary solution may address an immediate operational need, it does not necessarily increase an organisation's ability to understand and control the underlying technology. On the other hand, developing software internally or

contributing to open-source projects can strengthen expertise, improve technical understanding and reduce dependency on external providers, as well as help build the critical mass of users and contributors needed for open-source projects to succeed.

This led participants to frame digital strategic autonomy more broadly than the origin or ownership of a product. From this perspective, open source provides organisations with an opportunity to build the skills and capacity needed to understand, maintain, modify and continue operating the technologies on which they rely. It also gives them greater flexibility when outsourcing, as they are not limited to the original software provider and can work with a broader range of companies with expertise in open-source solutions.

In addition to building capacity, open source can also provide flexibility where standard commercial solutions do not fully match operational needs or lack commercial viability due to the limited size of the market. This was illustrated with the example of humanitarian organisations operating under specific constraints, such as limited connectivity, geopolitical restrictions or export controls. Participants noted that open-source components can be adapted and combined to build highly specialised systems, without requiring organisations to purchase multiple proprietary modules or depend entirely on a single vendor.

While it provides several benefits, open source raises questions that go beyond adoption itself. If open source is already deeply embedded in digital infrastructures, it also requires adequate governance, maintenance and long-term support. The discussion thus highlighted several interconnected dimensions and challenges, including sovereignty, sustainability, trust, governance, and culture.

Making Open Source Sustainable, Trusted and Usable 03

3.1. Beyond Free Software: The Cost of Sustainability

Open-source software is often described as free. However, participants strongly challenged the idea that it comes without a cost. Software may be freely available, yet maintaining it securely and reliably still requires people, infrastructure, testing, updates and long-term support. The central challenge is therefore to ensure that open-source software receives a level of maintenance and support that reflects the criticality of the systems that depend on it, and ensure the continuity of this support over time.

This requires sustainable economic models for open source. Participants noted that companies, especially small and medium-sized enterprises (SMEs), which account for 99.8% of European companies,[1] can build viable activities and business models around open source without selling the software itself, for instance through maintenance, support, specific developments, software evolution and continuity guarantees. Major open-source projects may also rely on commercial actors and private capital. Open-source projects therefore operate both as community-driven common goods and as infrastructure sustained by economic activity. However, in both cases, the actual asset, i.e., the open-source software, remains freely available for further development.

This sustainability issue is perhaps the most important aspect for organisations with critical missions or unusual operating conditions. Humanitarian organisations were once again cited as an example: they may rely on open source for flexibility and independence, but they still need reliable support and continuity to keep essential operations running.

The comparison with proprietary software also often leads to misleading conclusions about a practical trade-off. Proprietary solutions are often perceived as more attractive because they typically come with bundled support and services, while open-source software is assumed to require significant internal expertise and effort, even when licensing costs are minimal or non-existent. However, this distinction is not necessarily accurate. ***One of the strengths of open-source software is that support and maintenance can be sourced from multiple vendors, maintainers, and organisations, reducing dependency on a single provider and contributing to its long-term sustainability.***

At the same time, open source can be viewed as a contributor to resilience precisely because it is not tied to a single provider or single maintainer. If one specific project is discontinued, forks or alternative implementations may continue to exist and evolve. This does not remove the need for sustainable maintenance, but it reduces the dependency on the continuous existence and maintenance of one single stakeholder.

3.2. Building Trust Without Creating Barriers

Trust appeared throughout the discussion as a central issue. Open code provides transparency and gives users the possibility to fork, inspect, modify, and even influence development directions. However, openness alone does not guarantee that a project is secure, actively maintained, or suitable for critical use. Additional mechanisms are therefore needed to help organisations assess the level of trust that can be placed on an open-source solution. The challenge is then to provide users with sufficient assurance without

1. Annual report on European SMEs 2024/2025 - Publications Office of the EU. Available at: https://op.europa.eu/en/publication-detail/-/publication/2073ad00-3521-11f0-8a44-01aa75ed71a1/language-en

imposing requirements that small organisations, projects and communities cannot realistically meet.

Certification and conformity assessments were discussed as possible trust mechanisms, but participants also highlighted their limitations. These processes can be costly and slow, potentially discouraging innovation or creating disproportionate difficulties for smaller projects. The question of who should bear these costs is particularly important when widely used open-source software is maintained by communities rather than conventional commercial vendors. Participants suggested that certification approaches could evolve to better reflect the open-source development model, for example by making it easier to reassess only the components that have been modified rather than repeating an entire assessment after each release. More broadly, the discussion pointed to the need for trust mechanisms that are transparent, affordable, and able to evolve alongside the software they assess.

With the newly released Cyber Resilience Act (CRA), this issue has been partially solved by placing responsibility for compliance on the entity commercialising the software. However, as a downside, third-party certification that is imposed by CRA in some cases may create additional costs that can be particularly heavy for SMEs. This issue also extends to regulation and standardisation. Open-source developers and SMEs may have fewer resources to deal with complex compliance requirements than large companies. Participants therefore highlighted the need to balance stronger cybersecurity requirements with the capacity of smaller actors to implement them.

The Cyber Resilience Act adds an important element to this discussion by clarifying responsibilities around products with digital elements. Its treatment of open source is more nuanced than requiring all open-source software to be certified: free and open-source software that is not supplied in the course of a commercial activity is generally outside the CRA's manufacturer regime, while manufacturers placing open-source products on the market and certain open-source software stewards are subject to specific obligations. The CRA also establishes conformity-assessment requirements depending on the type and risk category of the product.

Greater trust in open source will require more structured assurance mechanisms, but these mechanisms need to remain proportionate to the resources and operating models of open-source projects. Stronger security and accountability should not come at the cost of excluding smaller actors or making continued open-source development unnecessarily difficult.

3.3. Open Source is Not Enough: The Role of Open Standards

Participants highlighted a contradiction between encouraging open-source development while important standards remain behind paywalls or embedded in complex standardisation processes, thus

creating the need for dedicated staffing, which is often lacking in SMEs. Open source and open standards were therefore presented as closely connected. Making source code available does not necessarily reduce dependency if the standards needed to build interoperable solutions remain difficult to access and implement, particularly for smaller organisations and open-source projects.

Interoperability was another central part of this discussion. Open-source implementations were seen as supporting interoperability because different actors can implement, test, and improve common standards openly. By contrast, participants criticised proprietary ecosystems that create "walled gardens" or modify standards in ways that make products work best within a single vendor's environment. Such practices can reinforce technological lock-in and reduce users' ability to move between solutions. In this area, regulation is still lagging significantly behind.

Digital strategic autonomy thus requires both open source and open standards. Reducing technological lock-in depends not only on access to source code, but also on ensuring that standards are accessible, interoperable and realistically implementable by smaller companies and open-source communities. Also, new business models that support open source are a critical success factor.

3.4. Sustaining the People Behind Open Source

Open-source communities were described as a core part of the model itself. Communities' contributions can therefore not be treated as an unlimited or self-sustaining resource. Contributors may be motivated by curiosity, learning, professional interest, recognition or paid work, while companies may finance employees to contribute to projects that are important to their own operations. Open source can therefore combine voluntary contribution, professional activity and a more value-driven or humanist approach to knowledge sharing.

Maintaining such communities requires active governance. Participants compared it to managing a shared playground: projects need to remain open enough to attract contributors, while still managing disagreements, behaviour and practical constraints. Legal and geopolitical restrictions can also limit participation, particularly where dual-use rules or export controls create unintended barriers. The broader point was that communities are built around people first, and that legal and governance mechanisms should support participation while protecting key control points.

Communication and visibility are also part of community sustainability, but are currently lacking in many open-source initiatives. Participants stressed that marketing is not separate from open

source development, but one of the ways projects attract contributors, maintain engagement, and create a shared identity while naturally making the open-source alternatives known. This can include regular communication on releases and ongoing work, realistic roadmaps, recognition mechanisms, gamification, bug bounties, or even simple community-building elements.

Forks were also presented as a normal and potentially valuable part of the open-source model rather than a sign of fragmentation. They can enable experimentation, testing and alternative development paths. Where useful ideas emerge, these can later be reintegrated into the original project. In this sense, forks can contribute both to innovation and resilience, provided that the resulting ecosystem remains manageable.

Finally, the discussion also pointed to the particular role of reputation. In open-source communities, reputation can function as an important form of value alongside money. Contributors and organisations build credibility through what they share and contribute, a process that can take years, while financial resources remain necessary to keep projects operating and to support professional involvement.

Open-source communities should be treated as part of the infrastructure that makes open source viable. Sustaining open source therefore requires more than just maintaining code: it also means supporting maintainers and contributors, keeping communities active, creating incentives to contribute, and providing the governance needed to manage openness over time.

When Automation Targets Open Collaboration

04

During the session, participants identified two main ways in which artificial intelligence (AI) is already affecting open-source communities. First, attackers can use AI to generate legitimate patches and contributions at scale, creating opportunities to introduce vulnerabilities under the guise of helpful participation. Second, AI can produce large volumes of low-quality code or irrelevant vulnerability reports, forcing maintainers to spend time separating genuine issues from noise. High-profile projects may be particularly exposed because of the attention they attract.

This creates an asymmetric problem. AI acts as a force multiplier for attackers, while maintainers remain a scarce human resource and often lack the manpower to investigate every submission or report. The concern is

therefore not only the quality of individual AI-generated contributions, but the cumulative pressure they can place on community processes and review mechanisms.

Participants were also cautious about relying on defensive AI as the main response. Automating more of the review process may help in some cases, but it can also create an escalating cycle of automated attack and automated defence, while potentially making participation more difficult for legitimate contributors. As one participant put it, this would be “fighting fire with fire”.

The forum therefore raised a broader governance question: how should open-source projects adapt when the community processes designed to encourage open participation can themselves be exploited through automation? Participants acknowledged there is not yet a clear solution.

Protecting open source will require not only better technical solutions, but also stronger governance and review mechanisms that can absorb higher volumes of automated activity without discouraging legitimate contribution.

Key Takeaways

The forum highlighted that open source should be treated as a strategic capability rather than simply as a low-cost alternative to proprietary software. It contributes to digital strategic autonomy by helping organisations retain control over the technologies they use through the ability to understand, maintain, modify, contribute to, and continue operating them independently. In that sense, sovereignty, or digital strategic autonomy, is not only about where technology comes from, but also about whether sufficient skills and capabilities remain available to use it independently.

At the same time, open source is only sustainable if the ecosystem around it is supported and supportive. Software may be freely available, but maintenance, testing, security, support, and continued development require resources. This makes viable business models, commercial investment, and long-term support mechanisms important, particularly for widely used or critical projects. The people behind open source are equally important: communities and maintainers should be considered part of the infrastructure that keeps these technologies operational.

Trust is another condition for wider adoption. Transparency and access to source code do not automatically guarantee security or reliability. Certification and other assurance mechanisms can help, but they need to remain proportionate and affordable so that they do not exclude SMEs, smaller projects or slow innovation. The same applies to standards: open source alone cannot reduce technological dependency if the standards it relies on remain inaccessible for developers or difficult to implement. Open standards and interoperability are therefore part of the same sovereignty discussion.

Overall, the discussion pointed towards a broader cultural shift. Open source should be seen less as an alternative technology choice and more as a long-term capability model. If Europe wants to rely on it for cybersecurity resilience and digital strategic autonomy, it also needs to support the skills, communities, business models, standards, regulations and trust mechanisms that make the ecosystem viable over time.

Recommendations and Action Points

01. Treat open source as part of critical digital infrastructure. Public and private organisations should **identify where they depend on open-source components** and reflect this dependency in resilience, security and continuity planning, as well as commercial decision-making.

02. Invest in internal capability, not only software acquisition. Organisations should develop the skills needed to **understand, maintain and adapt the technologies they rely on**, and acquire an understanding of the external actors who could support them with open-source transition.

03. Provide direct support to maintainers and open-source communities. Maintainers should be recognised as part of the infrastructure behind open source.

04. Develop proportionate trust and assurance mechanisms. Certification and other assurance approaches should provide meaningful guarantees without imposing costs and processes that smaller projects cannot realistically absorb. This should be taken into account when developing EU regulations.

05. Improve access to open standards and standardisation processes, which should be open to everyone. Open-source projects and SMEs should be able to implement relevant standards without disproportionate financial or administrative barriers.

06. Use interoperability as a criterion when selecting and designing solutions. Organisations should favour solutions that implement open standards and allow them to exchange data, integrate components and change providers without disproportionate costs or technical barriers.

07. Adapt community governance to AI-driven abuse. Projects should establish clear contribution guidelines and strengthen processes for reviewing code and vulnerability reports, helping maintainers manage automated submissions while preserving access for legitimate contributors.

08. Promote open source policy as a long-term capability model. European open source policy should go beyond encouraging adoption. It should **connect skills development, standards, funding, community support, assurance, and sustainable business models** so that open source can contribute meaningfully to digital strategic autonomy.

Thank you for reading. We hope these insights inform your work and encourage further dialogue on cybersecurity governance.

Thank you to our participants, Advisory Board and partners for sharing their expertise, **and to you for taking these discussions forward.**

nc3.lu
National Cybersecurity Competence Center
LUXEMBOURG

IN COLLABORATION WITH

Luxembourg House of Cybersecurity

LUXEMBOURG CYBERSECURITY FACTORY