Next Generation Internet 2025

A study prepared for the European Commission
DG Communications Networks, Content & Technology

Disclaimer

By the European Commission, Directorate-General of Communications Networks, Content & Technology.

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

Printed by the Publication Office in Luxembourg

Luxembourg: Publications Office of the European Union, 2018

Print	ISBN 978-92-79-86467-4	doi:10.2759/108457	KK-02-18-778-EN-C
PDF	ISBN 978-92-79-86466-7	doi:10.2759/49503	KK-02-18-778-EN-N

Next Generation Internet 2025

A study prepared for the European Commission
DG Communications Networks, Content & Technology

Authors

Michiel Leenaars – NLnet Foundation

Clementine Valayer – Gartner

Catherine Peyralbe – Gartner

Kristian Billeskov – Gartner

Marc Gauw – NLnet Foundation

Internal Identification

Contract number: 30-CE-0850616/00-55

SMART Number: SMART 2016/0033

Table of Contents

Abstract/Executive Summary

English

This report consolidates the outcomes of the study on the Next Generation Internet (NGI) 2025, SMART 2016/0033. It presents the:

- Technological analysis on Next Generation Internet future key technologies and research topics explaining the technical issues involved, based on the current gap today
- Key research communities and actors
- Impact of the research topics on the drivers for change which construct the Vision for an NGI
- Benefits linked to the research topics and the potential risks of not addressing them
- Recommendations to shape the programme for a Next Generation Internet Initiative based on specific selection criteria

The proposed NGI research topics for the H2020 programme are:

- Initiating trustworthiness
- Service portability and data decoupling
- Architecture renovation

The proposed NGI research topics for the Horizon Europe programme are:

- Resilient Internet Services
- Unbiased and privacy-respectful discovery of content and services
- Internet Hardening
- Securing end-user rights, protection and reputation
- Verification, accountability and automation mechanisms
- Provide end user friendly transparency mechanisms
- Promote freedom of use
- User empowerment through freedom of choice
- Greening the Internet
- A maintainable Internet
- Optimisable, reusable and reliable open hardware

Français

Ce rapport présente les résultats de l'étude sur l'Internet de la Prochaine Génération Internet (NGI) 2025, SMART 2016/0033:

- Analyse technologique des futures technologies clés du NGI, et les thématiques de recherche expliquant les problèmes techniques en jeu, sur la base de la lacune actuelle,
- Communautés et acteurs clés,
- Impact des thématiques sur les moteurs du changement qui construisent la vision du NGI
- Bénéfices liés aux thématiques et les risques d'inaction
- Recommandations pour façonner le programme NGI avec des critères de sélection précis.

Thématiques de recherche NGI proposées pour le programme H2020:

- Initier la crédibilité
- Portabilité du service et découplage des données
- Rénover l'architecture

Thématiques de recherche proposées pour le programme Horizon Europe:

- Services Internet résilients
- Recherche impartiale et respectueuse de la vie privée du contenu et des services
- Durcissement de l'Internet
- Sécurisation des droits, de la protection et de la réputation de l'utilisateur final
- Mécanismes de vérification, de responsabilisation et d'automatisation
- Mécanismes de transparence conviviaux pour l'utilisateur final
- Promouvoir la liberté d'utilisation
- L'autonomisation des utilisateurs par la liberté de choix
- L'Internet vert
- Un Internet maintenable
- Matériel informatique ouvert, optimisable, réutilisable et fiable

Deutsch

Dieser Bericht konsolidiert die Ergebnisse der Studie zum Next Generation Internet (NGI) 2025, SMART 2016/0033. Es präsentiert die:

- Technologische Analyse der Schlüsseltechnologien und Forschungsthemen der nächsten Generation des Internets, die die technischen Probleme auf der Grundlage der derzeitigen Lücke erläutern
- Wichtige Forschungsgemeinschaften und -akteure
- Auswirkungen der Forschungsthemen auf die Treiber des Wandels, die die Vision für eine NGI aufbauen.
- Vorteile im Zusammenhang mit den Forschungsthemen und die Risiken, die enstehen könnten, wenn diese Themen nicht angegangen werden
- Empfehlungen zur Gestaltung des Programms für eine Internet-Initiative der nächsten Generation auf der Grundlage spezifischer Auswahlkriterien

Die vorgeschlagenen NGI-Forschungsthemen für das H2020-Programm:

- Vertrauenswürdigkeit herstellen
- Serviceportabilität und Datenentkopplung
- Renovierung der Architektur

Die vorgeschlagenen NGI-Forschungsthemen für das Horizon Europe-Programm:

- Widerstandsfähige Internet-Dienste
- Unvoreingenommene und datenschutzfreundliche Entdeckung von Inhalten und Diensten
- Internet-Härtung
- Sicherung der Rechte, des Schutzes und der Reputation von Endnutzern
- Überprüfungs-, Rechenschafts- und Automatisierungsmechanismen
- Bereitstellung benutzerfreundlicher Transparenzmechanismen
- Förderung der Nutzungsfreiheit
- Ermächtigung der Nutzer durch Wahlfreiheit
- Ökologisierung des Internets
- Ein wartbares Internet
- Optimierbare, wiederverwendbare und zuverlässige offene Hardware

1. Introduction

1.1. Aim of the document

This document consolidates the effort in the study conducted towards the Next Generation Internet 2025, SMART 2016/0033. It presents the outcome of the study:

- the technological analysis on Next Generation Internet future key technologies and research topics explaining the technical issues involved, based on the current gap today
- the main research communities and key actors
- the impact of the research topics on the drivers for change which construct the Vision for a Next Generation Internet
- the benefits linked to the research topics and the potential risks of not addressing them
- recommendations to shape the programme for a Next Generation Internet Initiative with selection criteria.

1.2. Reader

- **Section 1** (this section)
  It introduces the aim of the document,
  - describes the structure of the information presented
  - places it in context of the complete study.
- **Sections 2 and 3**:
  The technological analysis on Next Generation Internet future key technologies has led to two sets of proposed research topics, developed in two separate sections:
  - the research topics proposed for the upcoming research calls in the **current H2020 programme** with detailed sections on the reasons and ways to approach the solutions
  - the research topics proposed for the NGI Programme implemented in the upcoming **Horizon Europe Research programme** with a section proposing potential ways to approach the solutions, knowing that the aim of the research is to innovate and that these calls will be made in the future when technology will have evolved offering other potential solutions
- **Section 4**: Recommendations for the NGI Programme
  This section presents recommendations for optimising the NGI programme through specific selection criteria for the projects proposed and for the intermediaries which will be implementing the calls with external stakeholders. In addition a set of recommendations are made with regards to making sure the NGI has a coherent and functionally adequate intervention logic.
- **Annexe 1**: Glossary
  This section presents a short description of the communities and organisations which are listed in the proposal calls, as well as explanation of some technical terms used in the document.
- **Annexe 2**: EC Policy areas
  This section lists the EC policy areas which are referred to in the proposal calls

1.3. Context of this document: the Vision for a Next Generation Internet and the drivers for change

This report is the final report of the study which earlier delivered a Vision for the Next Generation Internet. The Vision is structured on the drivers for change for a Next Generation Internet identified in the study. The Vision text is presented below, as it provides the strategic direction for the research topics:

An Internet of Human Values

Resilient. Trustworthy. Sustainable.

The overall mission of the Next Generation Internet initiative is to re-imagine and re-engineer the Internet for the third millennium and beyond. We envision the information age will be an era that brings out the best in all of us. We want to **enable human potential**, mobility and creativity at the largest possible scale – while dealing responsibly with our natural resources. In order to preserve and expand the European way of life, we shape a value-centric, human and inclusive Internet for all.

These important ambitions need a solid technical foundation to build on. The legendary robustness of the Internet must become actual reality in the Next Generation Internet. A massive global fleet of connected devices is on its way to enhance and control our homes, factories, offices and vehicles. Technology is embedded in concrete, circling in space and is increasingly entering the intimacy of our human bodies. The Next Generation Internet has to be both highly adaptive and unrelentingly **resilient**. Whatever companies or parts of the network go down by some natural or other disaster, the effects on us should be close to zero.

There is another essential dimension to trust, which lies above physical availability. We need a transparent technological environment, that is completely **trustworthy**. The architecture, governance and policies structure how entire societies and economies interact. By design it should protect free speech and private enterprise and much more. The Next Generation Internet is to be designed to avoid any bias or systematic abuse of global trust in the Internet. It shall be a true global commons, rising above international politics and competition. It will guarantee the safety of citizens and strengthen the health and autonomy of our markets and societies across borders.

The enduring success of the Internet lies in permission-free innovation, openness and interoperability. The Next Generation Internet is set up to empower, to unlimit our choices. It fosters diversity and decentralisation, and grows the potential for disruptive innovation. This extends far beyond the technical realm. The Next Generation Internet will achieve a **sustainably open environment** for our cultures and economies, celebrating our values and promoting creativity and well-being.

Let's re-invent Internet to reach the full human potential, for all generations.

The drivers for change which structure the text of the vision are:

- Creativity and human potential enabler
- Resilience / Reliability
- Transparency/ Trustworthiness
- Sustainability/ Openness

Each research topic is assessed on the number of drivers for change it supports, ensuring that the outcome of the research contributes to the Vision of the NGI which is focused on human values.

1.4. Research topic template

Each section presents the research topics with the following structure:

- Challenge
- Benefits
- Communities / problem owners
- Resource planning
- NGI Drivers for change
- Type of efforts and policy aspects
- Type of Action
- Risks of not addressing this topic

The text below presents a description of each of the topics in the structure.

Title

Challenge

The analysis section provides a description of the specific challenge from a user's perspective that the outcome of the technological analysis addresses.

Benefits

The benefits section describes the expected benefits from a user's perspective, of the funded research, and they are described in alignment with the charter of fundamental rights of the European Union.[1]

Communities/problem owners

Identification of the stakeholder communities which are (most directly) relevant to be engaged in the call. These communities are listed with their acronyms, and a detailed table in Annexe 2.

Resource planning

This section presents a high level estimate, on a scale of 1 to 5, of:

- *the phasing of the research call, when in the overall phasing logic of all the proposed topics should this one be phased so that coherence is achieved in terms of dependencies. Some aspects should be covered before others can build on them.*
- *the required effort, in a relation to all the proposed research calls on the list.*

Phasing	■□□□□	Required effort	■■■□□

NGI Drivers for change

Each research topic is assessed on the number of drivers for change it supports. This is done with two numbers:

- *the number of drivers impacted, which gives a view on the breadth of impact that the research potentially has*
- *the total of the level of impact on each driver, which gives a view on the depth of impact on change the research potentially has*

Resilience / Reliability	■■■■■	(5/5)
Transparency/ Trustworthiness	■■■■■	(5/5)
Sustainability/ Openness	■■□□□	(2/5)
Creativity and human potential enabler	■□□□□	(1/5)
Number of drivers impacted: 4	Overall impact on change:	13

[1] http://www.europarl.europa.eu/charter/pdf/text_en.pdf

Type of efforts and policy aspects

This section highlights which specific type of effort is relevant for this research topic. The type of effort is mentioned because of its relation to the efficiency of the funding. Some funding can relate to research, and other funding needs to relate to the actual implementation of the solution, its development (as in Research and Development activities). Other funding can relate to activities of maintenance of existing systems supporting the Internet or standardisation activities to ensure effectiveness of the research.

Research effort	Whether or not this requires new scientific research to provide fundamental building blocks
Development effort	Whether or not this requires a serious *software development* effort to convert new scientific building blocks into (open source) technology that can actually be deployed universally in the Next Generation Internet Effort
Maintenance and QA	Whether or not there is a significant amount of technical debt and/or serious security or scalability issues which require a serious *software engineering* effort to bring current building blocks in line with the Next Generation Internet Effort
Standardisation effort	Whether new internet or web standards will need to be established (with everything that entails) to make the overall intervention successful.

This section also highlights if the research would benefit from new policy measures to be impactful. It points to the need for significant educational efforts for the outreach of research outcomes to be maximized. The research may also impact some areas which are governed by policy so this section also lists which policy subjects[1] are relevant.

Requires new policy measures	Whether or not there is the need for legal intervention to restore the functioning of the market, in addition to the technology developed within the call.
Significant educational effort required	Whether or not education at large scale is a necessary component of the effort.
Existing policy subject impacted	This lists the policy subjects which are impacted by addressing or not addressing the topic. The policy categories are the twenty currently active EU Legislation topic categories in EUR-Lex complemented with the EC Digital Agenda. See *Annexe 2: EC Policy areas* for the complete overview of these 21 topics.

Type of Action:

This section presents what type of action is relevant for the research topic: Research and Innovation Action (RIA), Coordination and Support Action (CSA).

Risks of not addressing this topic

This section presents the risks if this topic is not addressed, if the situation stays as it is today.

[1] source: EU Legislation http://eur-lex.europa.eu/browse/directories/legislation.html?classification=in-force

2. Draft NGI Research Topics H2020 Programme

This chapter contains three proposed calls to be launched within the current H2020 framework.

These are 'cascading' calls, where suitable intermediaries will enable actual researchers and developers to do the work identified. Note that the size and timing of these calls were fixed before the launch of the study, and therefore these are considered a given.

For Horizon Europe and beyond, other designs can and should be considered to achieve the goals of the NGI Initiative. More about this can be found in chapters 3 and 4.

2.1. Proposed call I: Initiating trustworthiness

Challenge

If we want *everyone* to use the internet to its full potential without holding back, the internet cannot be partisan. This universal 'neutrality principle' lies at the heart of the global trust in the internet, as it is essential for maintaining sovereignty at the level of nation states and securing democratic ownership of the digital society. Trust is only sustainable if it the technology is trustworthy to begin with. The goal is to construct a minimal, trustworthy set of vetted core technologies ("trusted computing base") that can be relied upon by all users of the internet. This is done by identifying existing or creating new components as well as identifying and deprecating non-trustworthy elements. This requires applying severe scrutiny to key 'commodity' protocols and widespread implementations. The built-in security of core networking components may be the only line of defence for many applications and services on top of the network. Through this call the NGI will help to significantly improve security transparency, meaning that users will have a better understanding of their overall security situation on the internet.

Benefits

- Establish a secure technological base that can be assumed reliable for all purposes.
- Convergence mechanism for all NGI subprojects to establish quality and deliver proven solutions to others.
- Transparency about guarantees on business continuity and social connectiveness.
- Contributes to professional culture required for internet as a mature strategic infrastructure.
- Systematic and comprehensive approach re-enables trust in the system.

Communities/problem owners

- Computer science (Software engineering, Security, Software quality, Formal proof, Code generation, Testing, AI) – IFIP, ACM
- Kernel communities (Linux, OpenBSD, FreeBSD, etc)
- IRTF/ISOC/W3C
- Static/Binary/Hardware Analysis
- (National and sectoral) CERT
- ENISA
- MITRE
- FOSSi, OpenCores
- FSF/FSFE/APRIL/..

Resource planning

Phasing ■□□□□ Required effort ■■■□□

NGI Drivers for change

Resilience / Reliability	■■■■■	(5/5)
Transparency/ Trustworthiness	■■■■■	(5/5)
Sustainability/ Openness	■■□□□	(2/5)
Creativity and human potential enabler (user centricity,...)	■□□□□	(1/5)

Number of drivers impacted: 4 Overall impact on change: 13

Type of efforts and policy aspects

Research effort	✓
Development effort	✓
Maintenance and QA	✓
Standardisation effort	✓
Requires new policy measures	No
Significant educational effort required	-
Existing policy subject impacted	8 Competition policy 13 Internal Market 15 Consumer Protection 19 Freedom Security 20 People's Europe Digital Agenda

Type of Action:

Research and Innovation Action (RIA)

Risks of not addressing this topic

- European industry, society and defence are exposed to espionage/data exfiltration and (covert) sabotage.
- Users start to avoid the internet because of chilling effects and lack of trust.
- Overall system fails due to cyber attacks exploiting newly discovered vulnerabilities.
- Investments in improving security are ineffective due to persistent weaknesses ('hole in the bucket')
- High profile European citizens (scientists, politicians, etc.) and their environment are vulnerable to targeted profiling and exploitation.
- Uncertainty about what technologies are safe leads to high overspending on some risks and underspending on others.
- Failure to reach the overall vision of the NGI.

Detailed background information

The Next Generation Internet is not just a functional enhancement or mere optimisation of the current internet. The NGI is a necessary high level effort to overcome a rather fundamental trust crisis, which the internet has been pushed into in 2013 after whistle-blower revelations from an American security agency contractor detailing major abuse and covert global exploitation of internet weaknesses.

Until that point in time, the internet had generally been considered a major contribution to humanity, empowering end users and spreading freedom and knowledge everywhere. The harsh facts about large scale security exploits completely altered the perspective of many in the industry on the state, and therefore of the future course of the internet. At the IAB plenary of the 88th IETF, American security expert Bruce Schneier remarked: "The Internet has largely been run as the United States benign dictatorship, because everyone kind of believed the United States was acting in the world's best interests. That's over".

In retrospect, from a security analysis perspective, the internet has allowed mass surveillance and security compromise capabilities at a global scale. From a policy and technology point of view the integrity of the entire system should currently be considered breached. The untrustworthiness of the current core architecture of the internet and many of its legacy infrastructure components is problematic. There are strong interdependencies across different realms related to the internet, such as the web, the mainstream

operating system market for desktop and mobile, content discovery and delivery, e-payments and hosting ("the cloud"). Action is needed to amend that complex situation.

Why

Regular users and even network operators find themselves unable to effectively counter intrusive behaviour by various actors, including private and extra-legal actors. For many the fundamental lack of trustworthiness is the key rationale for urgently pursuing a Next Generation Internet. Succinctly put: we need trust built from the ground up. Every technical primitive from the current internet needs to be re-evaluated in terms of the complete threat catalogue, as we cannot afford our multi-trillion euro economies and societies to not be able to trust the internet as we move forward.

We need a Next Generation Internet that – beyond any doubt – is dedicated to the public good, which is (re-)engineered and professionally audited to achieve solid trustworthiness and transparency in all aspects of its operation. The core networking components need to be clean without defects or backdoors: they may be the only line of defence for many applications and services on top of the network. For now, especially in case of critical or vulnerable applications, the security integrity of the network should not be treated as axiomatic and additional measures need to be taken with the costs and additional effort associated. This way the NGI will help to create security transparency, meaning that users are able to adequate grasp their overall security situation.

The amount of suspect technologies we cannot avoid to rely on to ultimately needs to be reduced to zero. This is a very significant but unavoidable task if future contamination is to be prevented. It requires a structured long-term approach where step by step core technologies are either proven to be secure (possibly after improvements) and can remain in use, or are replaced *in situ* with better solutions. The urgency of this effort cannot be overestimated, given the high economic and social stakes. The end result should be a growing set of essential internet technologies which can be fully trusted as building blocks for any purpose. In future calls, also key client environments such as browsers, (mobile) operating systems and processors will need to be scrutinized to regain control over these core technologies. Through regulation and creation of strong alternatives some of the appropriation of the technologies by dominant actors will need to be undone. Transparency about the remaining (potentially tainted) dependencies or lock-in where no certainty can exist is essential, as well as stimulating appropriate short-term mitigations.

What

In this call the NGI initiative is looking for contributions from the technical community that help establish an initial trusted base set for the most strategic internet technologies. This serves as a trustworthy joint starting point from the ground up for the NGI efforts that will follow.

It welcomes the most effective and thorough proposals to address this urgent topic. Expected topics include:

- open security proofs and other strong guarantees for the full integrity of vital open source components and technologies
- fast-tracking maturation (features, performance, backwards compatibility) of suitable drop-in replacements with such strong guarantees, in particular where this is more efficient than elevating the legacy solution to that situation (or where the legacy solution is proprietary, which precludes universal deployment).
- audits, fuzzing tests and other approaches to improve software quality of vital open source software and hardware components and technologies; including tools for firmware analysis.

- improving the security of code generated by code generators and parsers directly from technical specifications
- at the protocol level, the NGI welcomes proposals which will add and implement robust encryption or other relevant technical measures to existing standards. It should be possible to adopt at scale to immediately circumvent safety issues and to help protect privacy of users.
- identifying and addressing known and unknown issues in core internet technologies.

Where trust isn't sufficiently established, this should be clearly marked. It is a race against the clock to address as many weaknesses as possible inside protocols, software and devices– some which were created explicitly, others left intentionally. Note that this first call is primarily aimed at the very short term, catering predominantly to the most strategic technologies and quick wins.

The list of reliable (best practice) technologies should be actively maintained during the NGI. This is considered a pivotal aspect of the NGI initiative. Future calls will address the topic more thorough and fundamentally, e.g. through security by (re)design at the architectural level.

2.2. Proposed call II: Service portability and data decoupling

Specific challenge

Users need to be able to separate their content and data from internet-based software and services. This ability re-establishes the boundaries between content owner and service provider, allowing alternative and complementary services to be mixed and matched. Service portability and data decoupling go hand in hand to help achieve openness to new entrants by unlocking clustered service verticals that have achieved dominant market positions. The availability of quality generic alternatives for all important classes of internet services will provide an enormous boost towards development and user mobility. By introducing suitable microscale alternatives and interoperable standards that can be universally deployed, individual service providers are no longer a single point of failure and resilience will be significantly increased. By making data and identities usable and portable across services, users regain control and innovative new services are made possible. Citizens and businesses can benefit not only from best-in-class applications but also re-use data across application boundaries.

Benefits

- Increase competitiveness of European vendors
- Users can choose service providers and/or host services themselves
- Allow incremental innovation and diversity to cater for minority needs
- Launch a competitive ecosystem of strong solution providers with a level playing field
- Contribute to standardisation to reduce friction
- More resilience: huge increase of redundancy
- Possibility for bottom-up localisation in minority languages
- Inclusiveness/design for all for people with disabilities and special needs

Communities/problem owners

- GÉANT
- W3C
- IETF/ISOC
- IFIP
- ACM
- Indieweb
- RemoteStorage.io
- Federated Identity mgmt
- Software Testing
- Academic UI/UX research
- FSF/FSFE/APRIL/...
- EDRi
- EuroISPA/DHPA/Eurocloud
- Open source community

Resource planning

Phasing ■■□□□ Required effort ■■■□□

NGI Drivers for change

Resilience / Reliability	■■■■□	(4/5)
Transparency/ Trustworthiness	■■■■■	(5/5)
Sustainability/ Openness	■■■■■	(5/5)
Creativity and human potential enabler (user centricity,...)	■■■■■	(5/5)
Number of drivers impacted: 4	Overall impact on change:	19

Type of efforts and policy aspects

Research effort	✓
Development effort	✓
Maintenance and QA	✓

Standardisation effort	✓
Requires new policy measures	Yes
Significant educational effort required	-
Existing policy subject impacted	8 Competition policy 13 Internal Market 15 Consumer Protection 19 Freedom Security 20 People's Europe Digital Agenda

Type of Action:

Research and Innovation Action (RIA)

Risks of not addressing this topic

- Stagnation of overall innovation
- Vendor dominance due to Metcalfe's law creates single points of (significant) failure in each domain
- Lack of alternatives makes users vulnerable to targeted profiling and exploitation.
- European businesses are at an unfair competitive disadvantage.
- Failure to reach the overall vision of the NGI.

Detailed background information

The second topic service portability and data decoupling transforms market-dominant 'black box' internet services into universally available alternatives available to all as generic 'white label' building blocks that can be reused and adopted by anyone. This allows user-driven incremental innovation and safeguards openness and diversity by actively steering away from market monopolies. In addition, without the pressure to maximise profit, services can be cleaned from psychological manipulation, be made more efficient and better adhere to the ethical preferences of the user. It also allows to decouple the software people use with the data and social environment they use.

Service portability and data decoupling go hand in hand to help achieve openness to new entrants by unlocking clustered service verticals that have strong market positions. The availability of commons alternatives for important classes of internet services which would allow data to be decoupled will provide an enormous boost towards development and user mobility. Active countermeasures against market dominance and lack of choice and control in application domains critical to the users. By introducing suitable microscale alternatives, the monolithic dependency on individual service providers (including hyperscale giants) can be dissolved and resilience will be increased.

Why

Due to network effects, benefits of scale and other factors (including spillover from market positions in other services), monolithic internet services quickly result in a soft lock-in of the user community with one or a few companies. The overall (social) cost of switching providers becomes too high, which means users can no longer autonomously decide to leave because they are co-dependent on a group of peers they use the service with. At that point users are at the mercy of the supplier, even if that user is facing very unfavourable or even unethical treatment or the service is no longer satisfactory. In the common case where multiple services are combined from a single very large company, these effects are even stronger.

Users should be able to use services that have the best match with their needs, ethics and rights at any point. At the very least they should be able to switch providers without friction, and to choose the conditions under which their services are run and where their data is stored. But services and user needs

are not static, nor universal. Supporting broad social and cultural diversity is not a given, and economically marginal user groups can be victim of this if this is left to business considerations alone. And among service providers there is no incentive to standardise and lower friction of switching, partially because of immaturity but also predictably because the soft lock-in benefits current vendors.

Allowing users to decouple the data they create themselves from the companies providing or hosting software allows introduction of new services, as well as better segmentation of risks – benefiting security and privacy.

By creating technology commons for popular services as open source technologies, a number of significant benefits are unlocked:

- users can choose service providers and/or host services themselves
- allow incremental innovation and diversity to cater for minority needs
- launch an ecosystem of strong solution providers with a level playing field
- contribute to standardisation to reduce friction
- more resilience: huge increase of redundancy, local deployment possible in case of large scale internet downtime
- possibility for bottom-up localisation in minority languages
- inclusiveness/design for all for people with disabilities and special needs

What

The goal is to establish suitable mature technology commons for popular end user services as open source, which do no require on any individual company and have no switching friction cost . These 'commons services' as well as their data should be portable across instances, and should allows for the decoupling of data with the services provided. And they should be user friendly and secure.

Users are likely to have experience with functionality from proprietary suppliers which may depend on conditions which will not be available or do not make sense if there is no need to directly monetise the user. Solutions to create or reuse (non-proprietary) social graphs through federation or decentralisation and/or low interaction methods of will need to be investigated, because monolithic models cannot apply. This also requires research and development into different user interaction as well as the potential for more efficient and ethical technical designs.

All solutions should be available as open source, and should either be based on (or serve as a first step to) establishing open standards by allowing portability of software and data. Any popular type of internet/web service is eligible, for instance:

- internet calendaring
- large file sharing
- collaboration tools (such as collaborative editors)
- content curation and bookmarking
- secure messaging
- issue tracking/project management
- ....

In addition, generic contributions to establishing the infrastructure to distribute and facilitate frictionless switching are eligible as project proposals:

- remote storage and transfer of content separate from software provisioning
- solutions to reuse non-commercial social and business graphs
- delivery methods.

2.3. Proposed call III: Architecture renovation

Specific challenge

At the heart of the NGI is architectural evolution that improves upon legacy core protocols of the internet. Such architectural changes will have to be introduced in a way that doesn't unnecessary break anything. The complexity of designing a successful architecture upgrade is easily illustrated by the fact that over half of the life time of the internet has already been spent on the (arguably not very successful) move away from IPv4. Given the diversity of use cases of today's internet, there are diverging design considerations and (potentially non-overlapping) solution spaces for different challenges which need to be investigated. Adoption of new protocols can leave room for complementary solutions to cater for different circumstances and different trade-offs (for instance between resilience, scalability and energy efficiency). Significant effort will have to go into understanding and mitigating the many practical aspects of potential transition from the current internet. Architecture renovation is widely recognised as critically important for the long term, and can provide structural solutions to problems that can only be partially mitigated within the current architecture – and at significant cost.

Benefits

- Ensuring business continuity and social connectiveness.
- Increase operational efficiency of the Internet.
- Introduce new capabilities at the core of the internet, enabling further innovation.
- Replace suspect technologies with technologies that have security and privacy by design.
- Simplify new technology by being able to relegate responsibilities.
- Lower environmental footprint of internet technologies.

Communities/problem owners

- IETF/W3C
- Computer science (network research), e.g. IFIP, ACM
- GÉANT
- RIPE (+ other RIRs)
- CENTR
- DNS operators
- Kernel teams
- ISOC
- EDRi
- FSF/FSFE/APRIL/...
- EuroISPA/DPHA/Eurocloud
- EURO-IX

Resource planning

Phasing ■□□□□ Required effort ■■□□□

NGI Drivers for change

Resilience / Reliability	■■■■■	(5/5)
Transparency/ Trustworthiness	■■■■■	(5/5)
Sustainability/ Openness	■■■■□	(4/5)
Creativity and human potential enabler (user centricity,...)	■■■□□	(3/5)

Number of drivers impacted: 4 Overall impact on change: 17

Type of efforts and policy aspects

Research effort	✓
Development effort	✓
Maintenance and QA	✓
Standardisation effort	✓
Requires new policy measures	No
Significant educational effort required	-
Existing policy subject impacted	15 Consumer Protection 19 Freedom Security 20 People's Europe Digital Agenda

Type of Action:

Research and Innovation Action (RIA)

Risks of not addressing this topic

The entire NGI threat catalogue applies.

In addition:

- Loss of innovation capabilities and competitiveness due to unnecessary technological dependencies.
- Raising the overall cost of future upgrades to the core technologies of the internet (technical debt).
- Loss of diversity, privacy, autonomy and choice for users.
- Giving way to alternative next generation internet technologies incompatible with European values.

Detailed background information

As the third suggested topic, architecture renovation, investigates alternative and/or auxiliary core infrastructures. Unlike the laws of physics, the way the internet works is the result of human design. As such it can potentially be modified over time given the right approach. This call is meant for projects aimed at changing the underlying fabric of the internet and the web itself, as well as any research and tools to assist in the practical transition or migration to new or updated technologies. The intent is to fix the known fundamental architectural weaknesses in the lower layers of the internet and apply lessons learned – taking into account many attempted failures at 'clean slate internet' or simplistic protocol update efforts so far. Many fundamental issues with resilience and robustness can only be fixed at a systemic level, but the inertia to overcome is huge.

We urgently need to evolve the internet's capabilities as a system. The fragility and inflexibility of many parts of the internet has been known for decades. Many practical workarounds have been found meanwhile to cater for explosive demand. These workaround unnecessarily raise cost and complexity, and actually make matters worse. The overall situation has accumulated into a huge technical debt that is again circumvented in fragile ways, contributing significantly to the ossification of the internet. Now we do not only need to upgrade the original technology, but we need to also mitigate the damage caused by clever workarounds that are less temporary than anticipated.

Why

Rewriting the ground rules (what may be assumed about the technologies underneath) has a huge effect at a higher level. New ways of addressing that prevent spoofing as well as enumeration of the entire

internet – a distinct possibility in the IPv4 space – make it impossible to subsequently brute force attacks. This would for instance change the whole dynamics of currently persistent threats – such as distributed denial of service by botnets. Similar changes can be envisioned to address other key issues such as mass surveillance capabilities.

Beyond legacy core protocols known to be unreliable or untrustworthy in the light of whistle-blower revelations, or solving known problems, new protocols additionally open up entirely new avenues. The original protocols are decades old, and even the 'new' IPv6 is. Modern usage is completely different from the static setup of those days, and key features such as disruption tolerance (in the face of nomadic usage through mobile devices) should not be an afterthought. Research into infrastructure renovation is essential to facilitate the introduction of exciting new capabilities. The more fundamental the new characteristics, the further we may evolve the internet.

What

Projects within this call investigate fundamental contributions to solving the internet's challenges. They may question the whole technology stack, the only condition being that they are feasible in terms of technology roll-out and prove their potential to provide lasting answers in line with the NGI Vision. In some cases it will be possible to retrofit novel principles into today's internet, or to encapsulate current behaviour as an application of the future architecture. In other cases this will be wholly impossible or extremely inefficient. In that case, creating forward compatibility by for instance providing suitable abstractions and mechanisms at the level of end points could be helpful.

A beacon here is the need to address the existential threats from the NGI threat catalogue. This actually entails a number of different classes of desired features. However, additional challenges have already been identified, such as cost and energy inefficiency at large scale, opaqueness of the ecological footprint (some applications used by small constituencies already consume more energy than entire countries) and scaling problems.

Potential higher level design goals for alternative infrastructures are

- Confidentiality and privacy
- Auditable integrity
- Scope isolation of contingencies
- Redundancy and self-repair
- Disruption tolerance
- Smarter asset distribution
- Better real-time behaviour
- Energy efficiency

Improvements to the system have been proposed and even implemented with various degrees of maturity and success over the course of decades. The approach taken here to overcome the inertia is that infrastructure renovation takes into account how it should be retrofitted and/or introduced at internet scale. This means technologies should not just exist in a paper, a technical specification at the IETF and a few patches in a software repository and a test run on an infrastructure test bed in a lab. Their claims and compatibility should be tested in every possible situation in an automated manner, through e.g. continuous integration . Investing in maintainability is vital to achieve that means – without a strong global deployment strategy inside operating systems, routers and management software, alternative infrastructures do not stand a chance. In addition to such deployments, providing adequate fallback mechanisms is a priority.

3. Draft NGI Research Topics Horizon Europe

3.1. Resilient Internet Services

Specific challenge

Creating a modern Internet infrastructure with connections and services intelligent and flexible enough to be able to avoid, repair and mitigate broken dependencies. Through practices such as connectivity redundancy (e.g. multi-homing), partitioning and smart asset distribution, the real-time dependency on a limited number of actors is reduced. The goal is to ensure high availability, resilience, openness and disruption tolerance.

Benefits

- Ensuring business continuity and social connectiveness
- More resilience: huge increase of redundancy
- Improve operational efficiency of the internet
- Lower the cost of operations
- Increase privacy by removing central 'vantage points'
- Improve disaster-readiness
- Level playing field for the market

Communities/problem owners

- W3C, Browser makers
- IETF
- GÉANT
- CENTR
- EURO-IX
- IFIP, ACM
- OS vendors (incl. mobile)
- EuroISPA/DPHA/Eurocloud
- Carriers/Access providers
- Kernel teams
- RIPE (+ other RIRs)
- FSF/FSFE, wider open source community

Resource planning

Phasing ■■□□□ Required effort ■■■□□

NGI Drivers for change

Resilience / Reliability	■■■■■	(5/5)
Transparency/ Trustworthiness	□□□□□	(0/5)
Sustainability/ Openness	■■■□□	(3/5)
Creativity and human potential enabler (user centricity,...)	■■□□□	(2/5)
Number of drivers impacted: 3	Overall impact on change:	10

Type of efforts and policy aspects

Research effort	✓
Development effort	✓
Maintenance and QA	✓
Standardisation effort	✓
Requires new policy measures	Yes
Significant educational effort required	✓
Existing policy subject impacted	13 Internal Market 15 Consumer Protection 19 Freedom Security 20 People's Europe Digital Agenda

Type of Action:

Research and Innovation Action (RIA)

Risks of not addressing this topic

- Large scale cascading of failures leading to societal disruption
- Growing dependency on a few operators which creates single points of failure
- Strengthening of dominant positions due to market effects
- Security weaknesses
- Monoculture
- Opaque use of resource distribution for data gathering

What

Projects within this call investigate how to modernize the Internet infrastructure with connections and services that are more intelligent in handling disruptions and more flexible and responsive in terms of operations. Some potential approaches to address this call are listed below:

- ### Partitioning/scope isolation

  The ability to segment parts of a network in such a way that issues in one segment have no side effects in other segments/parts of that network, which would allow for uninterrupted use outside of any affected areas.

- ### Redundancy through multihoming

  Combining multiple access networks (multihoming) Avoiding single points of failure and quality degradation by providing multiple independent alternatives, such as the ubiquitous ability to combine multiple access networks in parallel – often referred to as multihoming/multipath capabilities.

- ### High availability through smart assets distribution

  The real-time dependency on static content and software assets provisioned by individual organisations is a single point of failure and an asymmetric cost that can be mitigated at an aggregate level by different mechanisms to distribute and cache assets.

- ### High availability through automated advanced feature negotiation

  An important aspect of high availability is streamlining and automating how incidents are handled and mitigated across organisational boundaries, especially in parts or functions of services that are strongly connected. When operational conditions suddenly change (e.g. during emergencies or an attack), pre-negotiated fallbacks could result in increased responsiveness and quicker resolution.

- ## Countering cascading effects of system failures

  Many resources on the web and the wider internet are no longer self-contained, but have hard-coded dependencies on resources delivered by third parties, such as content delivery networks and cloud providers. These are used for critical features such as navigation. An outage somewhere in this chain can ripple an avalanche of unintended outages throughout many different systems. An example is the website of a registry that needs to be available to be used in case of emergencies to notify the administrators of a certain domain, but turns out to depend on 3rd party Javascript sources.

- ## Addressing the issue of global routing table size

  The number of prefixes in the global Internet routing table is increasing at an extremely fast rate, raising cost across the entire system. Solutions need to be found that either find alternative mechanisms that scale better or at least mitigate the effects of this growth.

3.2. Unbiased and privacy-respectful discovery of content & services

Specific challenge

Enabling unbiased and privacy-respectful discovery of content, services and metadata on the Web, also in a real-time local context. This will lead to higher trustworthiness of the Internet for the users, more openness of content and enhancement of creativity and human potential through alternative access to various types of content and services.

The internet and especially the web are constantly changing, as billions of people add, shift, modify and remove content and services. To find their way around, internet users heavily depend on a small set of active intermediaries such as search engines, social networks and platforms. This strong dependency carries a number of very significant risks: an intermediary may (either intentionally or non-intentionally) act as a gatekeeper (block certain things), exhibit an unfair (economical, political, social or other) bias and can intimately track, analyse and influence user behaviour. At internet scale looming dominance of a few large intermediaries (and the value system or lack thereof enforced their algorithms) is fed back into the decision process during creation and promotion decisions of content and services. This leads to a vicious cycle which reinforces dominance and as such has huge implications for the open nature of the Next Generation Internet. Allowing for bottom-up means of fine-grained discovery as well as shared metadata and other forms of enrichment and aggregation of content and services is essential to create alternatives.

Benefits

- Create a level playing field for digital services in Europe.
- Improve competitiveness of EU businesses.
- Improve transparency and choice of intermediary to consumers.
- Better support of cultural diversity.
- Support of education and knowledge.
- A better balance between benefits of and for intermediaries.
- A more fair and sustainable market in line with our values such as social security.
- Facilitating innovation for intermediary roles.
- Experimentation room for other economic models such as cooperatives.

Communities/problem owners

- W3C
- IETF
- IFIP, ACM
- FSF/FSFE, wider open source community
- OEM + after-market community
- GS1
- Search engines
- Browser makers
- Operating system vendors (incl. Mobile)
- CMS, ERP vendors

Resource planning

Phasing	■■■□□	Required effort	■■■□□

NGI Drivers for change

Resilience / Reliability	■■■□□	(3/5)
Transparency/ Trustworthiness	■■■■■	(5/5)
Sustainability/ Openness	■■■■□	(4/5)
Creativity and human potential enabler (user centricity,...)	■■■■□	(4/5)
Number of drivers impacted: 4	Overall impact on change:	16

Type of efforts and policy aspects

Research effort	✓
Development effort	✓
Maintenance and QA	✓
Standardisation effort	✓
Requires new policy measures	Yes
Significant educational effort required	✓
Existing policy subject impacted	08 Competition 13 Internal Market 15 Consumer Protection 19 Freedom Security

Type of Action:

Research and Innovation Action (RIA)

Risks of not addressing this topic

- Abuse of intermediary position by operators.
- Skewed competition and bias as regards the visibility of available digital services.
- Low visibility of highly relevant content and services.
- Algorithms favouring popularity leading to potential hypes (reinforcing fake news results etc.)
- No knowledge of what to look for (you don't know what you don't know)
- Price wars leading to impoverished markets.
- Censorship.

What

Projects within this call investigate how to achieve unbiased and privacy-respectful discovery of content and services. The aim of this call is to request solutions improving low-level discovery.

- ### Distributed market intelligence on the supply side

  Market mechanisms where the producers and service providers have ownership and control over flexible data models to describe their offerings and added value, which allow each to share rich information to be openly discovered by users leading to a diversity of aggregation mechanisms and business models.

- ### Bias-free discovery

  Solutions for unbiased and unmediated search and direct discoverability of services and content offered where possible. In particular the ability to retrieve neutral market information that disregards any psychometric user profiles, combined with the ability to expose any bias based on age, gender, educational level, social profile, etcetera.

- ### Mechanisms for privacy protection of search users

  Use of commercially available search tools can leak a great deal of private information about users, especially in case the search tools are cross-correlated with covert observational data ('analytics' and 'dark analytics') and in-service 3rd party data exposure (such as through advertisements from a remote server). Users should be able to discover products and services based on information they are willing to share.

- ### Discovery of 3rd party meta-information

  Just-in-time availability of relevant information from organisations such as consumer organisations and other consumers, without leaking any personal information from the user. This will strengthen the information position of users and would allow to better organise themselves.

3.3. Internet Hardening

Specific challenge

Achieve a trustworthy internet infrastructure that solves the fragility, lack of trust and confidentiality, and generally weak defence characteristics of the first generation internet. The goal is to ensure high availability, resilience, openness and disruption tolerance by providing a resilient, robust and secure routing and transport layer. Ubiquitous availability of tunnelling mechanisms can be provided to protect end users as an alternative to providing direct safe connections at the edges.

Benefits

- Creating a trustworthy environment enabling innovation.
- Ensuring business continuity and social connectiveness.
- The Internet is treated as strategic infrastructure, enabling trust in the system.
- Lower the cost of mitigating DDoS attacks and other cyber defense
- Increase privacy of users
- Increase the cost of untargeted mass surveillance
- Enable new types of services

Communities/problem owners

- IETF/W3C
- Computer science (network research), e.g. IFIP, ACM
- GÉANT
- RIPE (+ other RIRs)
- CENTR
- DNS operators
- Kernel teams
- ISOC
- EDRi
- FSF/FSFE/APRIL/...
- EuroISPA/DPHA/Eurocloud
- EURO-IX
- MITRE or a new European equivalent

Resource planning

Phasing	■■□□□	Required effort	■■■■■

NGI Drivers for change

Resilience / Reliability	■■■■■	(5/5)
Transparency/ Trustworthiness	■■■■□	(4/5)
Sustainability/ Openness	■■■□□	(3/5)
Creativity and human potential enabler (user centricity,...)	■■□□□	(2/5)
Number of drivers impacted: 4	Overall impact on change:	14

Type of efforts and policy aspects

Research effort	✓
Development effort	✓
Maintenance and QA	
Standardisation effort	✓
Requires new policy measures	Yes
Significant educational effort required	-
Existing policy subject impacted	13 Internal Market 15 Consumer Protection 19 Freedom Security 20 People's Europe

Type of Action:

Research and Innovation Action (RIA)

Risks of not addressing this topic

- The infrastructure can break because of high vulnerability, allowing cyber attacks.
- The internet is underutilised due to lack of trust by the users.
- Abuse by non-democratic governments threatens human rights
- Mass surveillance of citizens
- Continued exposure of communication patterns and social graphs
- Increased vulnerability to cybercrime
- Wifi4EU and similar 'free internet' offerings become a common attack vector
- Continued exfiltration of cryptographic key material cancels advances in traffic protections
- Users are vulnerable to targeted profiling and exploitation.
- European businesses have to deal with industrial espionage
- Failure to reach the overall vision of the NGI.

What

Projects within this call investigate solutions for Internet hardening. Some detailed issues providing potential approaches to address this call are listed below:

- ### Routing layer confidentiality

  The current routing mechanisms are known to be very weak against man-in-the-middle attacks and passive observation. They typically expose communication patterns to anyone in the path, even when end-to-end encryption is used. There are known solutions for this problem that need to be further developed and then upscaled. In the (limited) domain of optical networking/'light paths', the use of quantum networking should also be further investigated as a solution for even more confidentiality for e.g. back-haul.

- ### Improving high availability by countering/preventing spoofing and amplification attacks

  Rooting out spoofing and amplification attacks is a significant challenge. With a minimum of effort parts of the current internet can be weaponised to attack other parts: there are old internet protocols that are still in common usage which will happily answer every request they get sent with an answer that can be over 4000 times larger. As long as spoofing can still happen, this means that attackers have a huge advantage over those that have to keep their systems up and running. In some cases, this requires rewriting otherwise well-functioning protocols and software.

- ### Improve legacy equipment by improving network isolation and segmentation

  Inadequate isolation and/or network segmentation caused by legacy network equipment causes a threat to the overall health of the internet

- **Providing universal transport-layer security**

  Ensuring at the transport layer that Internet traffic is moving securely between end-points and thus simplify solutions for providing application-layer security

- **Counter natural and man-made disaster threats**

  Improve the resilience of the network against events that damage critical parts of the infrastructure, such as earthquakes, solar flares and floods. Nuclear explosions, acts of terrorism, vandalism and other forms of intentional and unintentional sabotage or failure which are the result of human action.

- **Countering problems caused by inadequate isolation/segmentation**

  The combination and/or proximity of different types of applications and user domains in a single infrastructure means that the risks of that combined system may end up as the sum of all risks. One submission pointed out a quote by a security manager: “In a relatively short time we've taken a system built to resist destruction by nuclear weapons and made it vulnerable to toasters.

- **Hardening the Internet towards cyber warfare**

  Disruption of the internet infrastructure of a region for military and political purposes is by now known as the fifth domain, next to land, sea, air and space. How do we limit the potential impact of cyber warfare and cyber conflicts?

- **Redesign existing standards to improve security**

  Standards developers sometimes overallocate capabilities to certain actors to satisfy edge cases, assumptions about cost or certain business interests, which can put users unnecessarily at risk. Tainted and suspect standards need to be replaced by hardened alternatives, not just in theory but in actual usage. Overpowered standards that are detrimental to user privacy and security – such as cookies, where the original engineers that created it already warned against allowing 3rd parties to use them – can only disappear when the original need is fulfilled by a minimal functional replacement that prevents further abuse.

- **Protecting users during nomadic access (e.g. public Wi-Fi)**

  Use of untrusted networks such as the upcoming WIFI4eu, or the Wi-Fi in a train station or coffee bar is a pervasive risk in the current generation of the internet. There is no mechanism for citizens to distinguish rogue networks from real ones. Updates to the technology are required, and once these are in place legacy technologies outside of the private home should be phased out – if necessary by means of regulation.

- **Protecting against industrial espionage**

  Industrial espionage is the theft of advanced technology from industry, academia and military through exploiting internet infrastructure weaknesses. Solutions protecting against espionage should be developed.

- **Provide end to end confidentiality of traffic metadata**

  The fact that machines are forwarding packets does not mean they should learn who is communicating with whom. IP datagrams leak this information, additional or alternative mechanisms are necessary to prevent loss of confidentiality.

- **Providing control and ability to verify routing paths**

  Routing paths should be verifiability and under control of the sender. End hosts might want to avoid packets being routed through adversarial or untrusted networks, or they might want to choose the most suitable path with regard to a specific metric (e.g., latency or bandwidth).

3.4. Securing end-user rights, protection and reputation

Specific challenge

Trust is the key driver for human interaction. Identity and reputation are characteristics which should be an intrinsic part of the internet infrastructure, yet any such unbiased shared infrastructure is lacking. Market-driven mechanisms in this area are opaque and predatory, and tend to reinforce already problematic market imbalance and unfairness. In addition these produce undesirable side effects such as passive profiling and exposure to corporate surveillance. In order to secure end-user rights, the NGI needs to create decentralised internet-wide identity mechanisms, distributed reputation options and ensuring viable means of extending end-of-life of software and software-enabled devices. The goal is to improve the trustworthiness of the Internet and the sustainability of software and devices making use of it, which builds the levels of trust for the Internet to be levered in innovation.

Benefits

- Consumer's identity protection on the Internet.
- Support the right to do business
- Supports the right to the integrity of the person
- Respect for private and family life
- Everyone has the right to respect for his or her private and family life, home and communications.

Communities/problem owners

- IETF/W3C
- GÉANT
- CENTR
- EDRi
- FSF/FSFE
- EuroISPA/DPHA/Eurocloud
- EURO-IX
- Financial institutions
- Member states
- (Computer) Science/Academia

Resource planning

Phasing 

Required effort 

NGI Drivers for change

Resilience / Reliability		(4/5)
Transparency/ Trustworthiness		(5/5)
Sustainability/ Openness		(4/5)
Creativity and human potential enabler (user centricity,...)		(4/5)
Number of drivers impacted: 4	Overall impact on change:	17

Type of efforts and policy aspects

Research effort	✓
Development effort	✓
Maintenance and QA	-
Standardisation effort	✓
Requires new policy measures	Yes
Significant educational effort required	-
Existing policy subject impacted	13 Internal Market 15 Consumer Protection 19 Freedom Security 20 People's Europe Digital Agenda

Type of Action:

Research and Innovation Action (RIA)

Risks of not addressing this topic

- Highly complex privacy issues, preventing widespread understanding and protection.
- Identity and reputation of users compromised, hindering citizens' and businesses' rights.
- Lack of technology adoption and diminished use because of user concerns.

What

Projects within this call investigate solutions for securing end-user rights, protection and reputation. Some potential approaches to address this call are listed below:

- ### Countering pervasive surveillance schemes

  Several long term programmes for pervasive surveillance dating back to the earliest days of the internet have meanwhile been exposed, most notably Edward Snowden. However, the threat model should take into account that not all capabilities are likely to have been revealed, and that other actors have also set up similar schemes.

- ### Distributed reputation

  Finding solutions to the distribution of reputation. As in real life, reputation provides additional trust – however, reputation should have reasonable dampening mechanisms to avoid reputation attacks.

- ### Decentralised internet-wide identity mechanisms

  The trustworthiness of the Internet needs improvement. One of the initiatives would be to provide decentralised internet-wide identity mechanisms. A better protection of users starts with the ability to distinguish users from each other.

- ### Ensure extended EOL to end-users

  Duty to update/mandatory open sourcing at the End Of Life of devices. Users should not need to throw out working devices, because the original vendor is no longer supporting security updates. Alternatively, full technical specifications could be published and any hardware or software locks present preventing installation of updates could be switched off.

- ### Naming system alternatives

  The DNS system is known to leak a lot of detail about the behaviour of users to third parties, including public DNS operators and Wi-Fi hotspot operators (these are known to be very unsafe, to anyone). DNS is regularly used as a tool of censorship and in some cases surveillance. A lot of customer premises equipment is unable to deal with modern DNS, leading to a lack of

upgradeability which is problematic. A dual strategy of hardening at the one end and shifting to fundamentally more secure and privacy-friendly solutions with a an adequate deployment strategy at the other end is recommended.

- Provide citizen protection against malicious business practices

  Stricter maintaining of existing laws and regulations protecting users can help promote alternative mechanisms that are more respectful to end user privacy. Business practices like Real-Time Bidding are in clear violation of the letter and intent of existing privacy regulations, and yet these practises continue to take place.

3.5. Verification, accountability and automation mechanisms for NGI

Specific challenge

The NGI initiative presents an unprecedented challenge of providing efficient accountability and security mechanisms for the operational NGI initiative with tamper-proof technical solutions such as security proofs, risk protection tools, as well as whistle-blowing options and accountability mechanisms. These solutions should ensure high availability of the NGI, counter issues such as sabotage or surveillance, and provide distributed trust mechanisms to remove single points of failure. Security solutions could also include mechanisms to encourage automating incident- and abuse-handling to further secure safe Internet use during operations. The goal is to improve the trustworthiness, reliability and sustainability of the Internet, enabling innovation.

Benefits

- Supporting safety of EU citizens and their data
- Ensuring business continuity and social connectivity
- Stable operation of the NGI initiative
- Increased trust in the NGI initiative will stimulate adoption
- Ability to investigate signals of corruption
- Avoid investing in technologies that are untenable
- Decrease future cost of security auditing by create verifiable trustworthiness that cannot be perverted
- Lower overall cost of deployment and maintenance while improving responsiveness

Communities/problem owners

- Software engineering, Computer Science (Security, Software quality, Formal proof, Code generation, Testing, AI, Network research) – e.g. IFIP, ACM
- IETF
- EuroISPA/DPHA/Eurocloud
- EURO-IX
- GÉANT
- RIPE (+ other RIRs)
- CENTR
- DNS operators
- Kernel communities (Linux, OpenBSD, FreeBSD, etc)
- Static/Binary Analysis
- FIRST, CERTS
- ENISA
- FOSSi, OpenCores
- FSF/FSFE/April

Resource planning

Phasing ■■□□□ Required effort ■■■■□

NGI Drivers for change

Resilience / Reliability	■■■■□	(4/5)
Transparency/ Trustworthiness	■■■■■	(5/5)
Sustainability/ Openness	■■□□□	(2/5)
Creativity and human potential enabler (user centricity,...)	■■□□□	(2/5)

Number of drivers impacted: 4 Overall impact on change: 13

Type of efforts and policy aspects

Research effort	✓
Development effort	✓
Maintenance and QA	✓
Standardisation effort	✓
Requires new policy measures	No
Significant educational effort required	-
Existing policy subject impacted	13 Internal Market 15 Consumer Protection 19 Freedom Security Digital Agenda

Type of Action:

Research and Innovation Action (RIA)

Risks of not addressing this topic

- Monoculture and potential monopolies on security aspects of internet infrastructure.
- Corruption of researchers will lead to back doors and vulnerabilities
- Continued weak defence against cyberattacks
- Exploitation of devices for botnets and cybercrime
- High consumer cost for replacing broken equipment
- The system is underutilised due to lack of trust by the users.

What

Projects within this call investigate solutions for verification, accountability and automation mechanisms for the NGI. Some potential approaches to address this call are listed below:

- ### Provide certified security proofs to end-users

  Security proofs (We are past the stage where a pretty design is satisfactory. The security of browsers and operating systems as the client side run environment of the Next Generation Internet should be subject to academic scrutiny)

- ### Contain digital spillover in physical world

  Mobile devices and wearable tech potentially leak undesired information about people other than their owner. How do we prevent such spillover in a machine processable way, so that people do not have to justify or explains themselves and can feel safe in the company of other people

- ### Protecting against industrial sabotage

  Industrial sabotage (Disruption and exploitation of internet weaknesses aimed at competing global regions and economic actors, aimed at giving the attacker a competitive edge)

- ### Accountability

  Identify solutions for implementing accountability principles.

- Distributed trust mechanism

  Given the inherent vulnerability of any single root of trust, there is a preference for distributing trust mechanisms to remove single points of failure, and finding ways to delegate trust in an auditable and controlled way.

- Technical baseline for devices (minimum exploit mitigation baseline for embedded systems)

  Make sure that R&D will not be wasted on platforms that do not offer future proofness with regards to exploit mitigation. such as Executable Space Protection (ESP), Code Memory Software Diversification, stack canaries and ASLR.

- Technical baseline for cryptographic functionality

  Make sure that the higher level technology aspects are not lost to low level hardware incapabilities, e.g. offer Secure Random Number Generation, Secure Key Storage and Cryptographic Acceleration.

- High availability through abuse handling

  An important part of maintaining high availability is streamlining and automating how incidents are handled across the network, especially in parts or functions of the network that are strongly connected. This make the overall system more secure, because it allow increased responsiveness to changing operational conditions, particularly in time of emergency.

- Hardware validation

  Methods to reverse engineer and measure actual hardware to verify the absence of any intentional or non-intentional flaws that could be abused for attack purposes.

3.6. Provide end user friendly transparency mechanisms

Specific challenge

Providing user-friendly accesses to transparency mechanisms, such as transparency on the security situation of a connection, background processes, data collected and observed or data retention. These mechanisms can also provide tweaking options empowering the user to define the security levels. This will lead to higher trustworthiness of the Internet with the effect of enabling innovation and creativity.

Benefits

- Supporting safety of EU citizens and their data
- Improving transparency to consumers
- Ensuring business continuity and social connectiveness
- User empowerment leading to higher innovation
- Ability to verify adherence to EU laws
- Level playing field between good actors and malicious actors

Communities/problem owners

- W3C
- IETF
- IFIP, ACM
- FSF/FSFE, wider open source community
- OEM + after-market community
- GS1
- Search engines
- Browser makers
- Operating system vendors (incl. Mobile, VR)

Resource planning

Phasing ■■■□□ Required effort ■■■□□

NGI Drivers for change

Resilience / Reliability	■■■□□	(3/5)
Transparency/ Trustworthiness	■■■■■	(5/5)
Sustainability/ Openness	■■□□□	(2/5)
Creativity and human potential enabler (user centricity,...)	■■■■□	(4/5)
Number of drivers impacted: 4	Overall impact on change:	14

Type of efforts and policy aspects

Research effort	✓
Development effort	✓
Maintenance and QA	✓
Standardisation effort	✓
Requires new policy measures	Yes
Significant educational effort required	✓
Existing policy subject impacted	13 Internal Market 15 Consumer Protection 19 Freedom Security 20 People's Europe

Type of Action:

Research and Innovation Action (RIA)

Risks of not addressing this topic

- Lack of knowledge leading to vulnerability of businesses and citizens relating to the abuse/predation of data
- Lack of trust regarding how data is handled, lowering the usage of the system and hindering innovation
- High cost of law enforcement in Digital single market.

What

Projects within this call investigate solutions for providing end user friendly transparency mechanisms.

Some potential approaches to address this call are listed below:

- ### Right to know about gathering of observational data

  Right to have insight into big data gathering (The user should be able to know exactly what observational data is being gathered, and who it will be sent to before it actually happens)

- ### Provide end-user transparency mechanisms for background processes

  Background process transparency: users should be able to easily inspect every background process in the technology they use.

- ### Provide end-user security transparency

  Users should be able to grasp the overall security situation of a specific connection.

- ### Provide transparent security for the end-user

  Open (user-defined and controlled) security (Allow users to easily override weak security settings of software vendors and and protect their communication with the level of protection the user himself deems necessary)

- ### Protecting users from malicious data observation

  Passive observation of users by companies without their explicit knowledge and consent, which includes storing the complete browsing history of users, location data, media consumption, shopping behaviour, cross-device identification of users, stealth identification of other users in the vicinity, undisclosed audio streaming for off-site analysis, persistent identifiers, etcetera)

3.7. Promote freedom of use of the NGI

Specific challenge

Ensuring fair access and freedom of use of the NGI. The safeguard of the NGI openness to new entrants is enabled by making it simpler to create services and by unlocking dominant positions in application domains strategically important to the users, which is hampering development and innovation. Freedom of use is ensured by mechanisms supporting open access, such as stimulating the offering of scalable shared mechanisms to support multi-cultural needs, like multilingual use and local content. This openness drives sustainability of the NGI while enabling diverse creativity and innovation.

Benefits

- Support the right to do business
- Level playing field for competition
- Cultural diversity
- Improve competition and innovation by lowering barriers of entry
- Improve inclusiveness
- Enable the spread of knowledge
- Decouple the service infrastructure from monopolistic actors

Communities/problem owners

- EuroISPA/ECO/DHPA
- Council of Europe
- National regulators
- Consumer organisations
- EDRi
- UNESCO IFAP
- Internet Society
- W3C
- IFIP, ACM

Resource planning

Phasing 

Required effort 

NGI Drivers for change

Resilience / Reliability		(3/5)
Transparency/ Trustworthiness		(3/5)
Sustainability/ Openness		(5/5)
Creativity and human potential enabler (user centricity,...)		(5/5)

Number of drivers impacted: 4 Overall impact on change: 16

Type of efforts and policy aspects

Research effort	✓
Development effort	✓
Maintenance and QA	✓
Standardisation effort	-
Requires new policy measures	Yes
Significant educational effort required	✓
Existing policy subject impacted	08 Competition 13 Internal Market 15 Consumer Protection 19 Freedom Security 20 People's Europe Digital Agenda

Type of Action:

Research and Innovation Action (RIA)

Risks of not addressing this topic

- Content available in only a few languages, hindering the wider spread of knowledge
- Emergence of monoculture
- Monopolistic landscape hindering the access to the Digital Single Market
- Hinder innovation potential of the data economy

What

Projects within this call investigate solutions for promoting freedom of use of the NGI. Some potential approaches to address this call are listed below:

- ### Provide common solution to multi-lingualism

  This maintainability not only concerns technical aspects, but also cultural – such as offering scalable shared mechanisms to support multilingual use, i.e. availability of ICT in every language – driven by the needs of the language communities rather than business decisions.

- ### Metalanguage for coding the Internet with a user-friendly interface

  The barrier to entry for normal people to create new services is still quite high. This solution explored addresses a way to easily "code" Internet sites and services for IT agnostic users.

- ### End-user capabilities with open spectrum

  The availability of enough end-user controlled radio spectrum allows for grass roots innovation and is vital for innovation and choice

- ### Mass education

  Explore innovative solutions for delivering mass education on online rights, privileges, trustworthiness, risks

3.8. User empowerment through freedom of choice

Specific challenge

Ensuring user empowerment through mechanisms allowing the choice of user profiles relating to browsing, security levels and access to content. These mechanisms include standard interaction patterns, enacting for example the right to be offline when using connected devices, as well as using safe content profiles or generic profiles for revealing personal information. Other mechanisms can relate to the right to encryption or domain isolation. This will lead to higher openness and trustworthiness of the Internet with the effect of enabling innovation and creativity.

Benefits

- Consumer's identity protection on the Internet
- Supports the right to the integrity of the person
- Respect for private and family life
- Improves trust in new technologies and supports innovation

Communities/problem owners

- W3C
- Computer science (markup languages, cryptography, declarative interaction) – e.g. IFIP, ACM
- Browser vendors
- Mobile OS creators
- OEM
- EDRi

Resource planning

Phasing 

Required effort 

NGI Drivers for change

Resilience / Reliability		(1/5)
Transparency/ Trustworthiness		(4/5)
Sustainability/ Openness		(3/5)
Creativity and human potential enabler (user centricity,...)		(4/5)

Number of drivers impacted: 4 | Overall impact on change: 12

Type of efforts and policy aspects

Research effort	✓
Development effort	✓
Maintenance and QA	-
Standardisation effort	✓
Requires new policy measures	Yes
Significant educational effort required	✓
Existing policy subject impacted	13 Internal Market 15 Consumer Protection 19 Freedom Security 20 People's Europe Digital Agenda

Type of Action:

Research and Innovation Action (RIA)

Risks of not addressing this topic

- No understanding of security issues and ways to protect oneself as a user
- Lack of trust in technology, hindering economic growth
- Loss of freedom (arbitrary use of data)

What

Projects within this call investigate solutions for empowering users through freedom of choice. Some potential approaches to address this call are listed below:

- ### Develop standard interaction patterns to allow declarative interaction

  Allowing to run unverified software on web pages poses a risk to the user. By standardising popular interaction patters, users only have to passively declare the desired interaction, and do not have to bother the user with permission to run unverifiable scripts on a web page.

- ### Implement safe content profiles for end users

  Safe (passive) content profiles (The original design of the web as a set of documents where can safely surf from link to link, has been lost over time due to the rise of demanding applications that appropriated the technology to get system agnostic interfaces. As a result, document are now no longer safe. When a user browses an unknown website, he or she typically grants the operator the same technical privileges as a bank or trusted software supplier would need – browser have not been given the native abilities to distinguish among known and unknown). Browsing the internet, the risk of abuse is very significant. Availability of a safe content profile (e.g.. return of the web document) would provide a subset of features that is known to be secure and passive, which would guarantee the end users are not attacked while they just want to read a document.

- ### Provide domain isolation between web sites

  Another part of securing the browser environment is by domain isolation: similar to how experimental operating systems like Qubes OS provide a very strict isolation between types of activities, the amount of observational data about a user between their use of different websites should be minimised unless the user explicitly makes the connection.

- ### Provide generic profiles for revealing personal information

  Sensor data deniability and firewalling (In browsers, mobile operating systems and even more in wearable tech there is a real need for users to be in control of what the sensors and application software inside their device are revealing about them to the outside, such as their location or life

habits. A user should be able to silence or randomise sensors, or to have her geolocation module (e.g. GPS, Galileo) give inaccurate data about her whereabouts to applications that do not need such intimate information.

- Ensure hardware protection from abusive monitoring

  Mandatory hard switches for embedded cameras and other devices (Cameras and microphones are particularly invasive, and a high profile target for abuse. Users should be able to physically switch off cameras and microphones they are not using, so that they can be 100% safe from the emergence of sudden software flaws or security glitches as well as undesirable business practises.

- Right to be IoT offline

  People should not be forced to use invasive technologies by their employer or other persons that have authority over them, and can identify when they are tracked and chose to be offline.

- Right to encryption for all

  Encryption is the single most important technological building block of internet security. Users should be able by law to encrypt any data and any communication with a mechanism they themselves trust.

3.9. Greening the Internet

Specific challenge

Providing transparency mechanisms on the environmental cost of the Internet, identifying and tagging which elements are the most resource-consuming and researching what would be the alternatives to improving energy efficiency, both locally and globally, on the Internet infrastructure and connected devices. The goal is to ensure sustainability of the Internet and of the economy relying on it.

Benefits

- Improve efficiency of digital services, including public services
- Protection of the environment
- Ensure sustainability of the Internet
- Lower the price of digital innovation and enable take-up
- Support businesses in implementing CSR

Communities/problem owners

- National governments
- FOSSI, OpenCores
- Hardware vendors
- Computer science (Software engineering, Code optimisation, AI, security researchers[1]), e.g. IFIP, ACM
- Kernel communities (Linux, OpenBSD, FreeBSD, etc)
- FSF/FSFE/APRIL + wider open source community

Resource planning

Phasing 

Required effort 

NGI Drivers for change

Resilience / Reliability		(5/5)
Transparency/ Trustworthiness		(5/5)
Sustainability/ Openness		(4/5)
Creativity and human potential enabler (user centricity,...)		(3/5)

Number of drivers impacted: 1 Overall impact on change: 4

[1] Note that energy saving features without proper countermeasures may in some cases result in increased vulnerability to side-channel attacks to cryptographic operations.

Type of efforts and policy aspects

Research effort	✓
Development effort	✓
Maintenance and QA	✓
Standardisation effort	✓
Requires new policy measures	Yes
Significant educational effort required	-
Existing policy subject impacted	15 Environment protection

Type of Action:

Research and Innovation Action (RIA)

Risks of not addressing this topic

- High resource consumption barrier to innovation and take-up
- Non-usable Internet in post-carbon economy
- Failure to meet international sustainability goals
- Missed business opportunities to establish new highly compute-intensive industries
- Inability to respond to crisis situations

What

Projects within this call investigate solutions for greening the Internet. Some potential approaches to address this call are listed below:

- ### Improve transparency of environmental cost of internet technologies

  "Greening" internet technology concerns the need to improve energy efficiency, both locally and at an internet level. Currently there is a significant lack of transparency of environmental cost, which should be urgently resolved given the vast scale of resource usage. This would include analysing the impact of e.g. blockchain implementations.

3.10. A maintainable Internet

Specific challenge

Provide a manageable Internet supporting efficient deployment of upgrades. This effort will increase the likelihood that the deployments are being implemented correctly, and with successful results. It aims at having a manageable and coordinated approach to get the needed deployments and upgrades on the Next Generation Internet by using realistic transition mechanisms, solving scalability issues, collecting feedback by real time data gathering, and encouraging the right network equipment upgrade capabilities and emergency response procedures. The goal is to ensure resilience, reliability, trustworthiness and sustainability of the NGI.

Benefits

- Lower costs at the project level by shared infrastructure and setup.
- Increased reusability of efforts and sharing of knowledge across and beyond projects.
- Increase the efficiency of the overall infrastructure.
- Improve transparency to and agency of the internet users.
- Increase responsiveness and availability of the Internet.
- Lower cost of deployment for users.

Communities/problem owners

- Computer science (Software engineering, Security, AI), e.g. IFIP, ACM
- OEMs, Hardware vendors
- Operating system vendors
- Research and Education Networks
- EuroISPA/ECO/DHPA
- FSF/FSFE/APRIL and the wider open source community
- FIRST, CERTs
- Software Heritage

Resource planning

Phasing 

Required effort 

NGI Drivers for change

Resilience / Reliability		(5/5)
Transparency/ Trustworthiness		(3/5)
Sustainability/ Openness		(4/5)
Creativity and human potential enabler (user centricity,...)		(1/5)

Number of drivers impacted: 4 | Overall impact on change: 13

Type of efforts and policy aspects

Research effort	✓
Development effort	✓
Maintenance and QA	✓
Standardisation effort	✓
Requires new policy measures	No
Significant educational effort required	✓
Existing policy subject impacted	13 Internal Market 15 Consumer Protection 19 Freedom Security 20 People's Europe Digital Agenda

Type of Action:

Coordination and Support Action (CSA)

Risks of not addressing this topic

- NGI projects do not benefit from each others results, and are unable to deal with overarching issues.
- Subprojects inside NGI will each invent different quality procedures and delivery.
- Reusability will be low and the resulting infrastructure remains unmaintainable and unresponsive.
- In the event of security breaches and operational failure of the Internet, there will be lower efficiency in fixing.
- Prolonged unavailability cannot be prevented due to lack of a shared upgrade mechanism.
- Lack of maintainability at the NGI level, unclear what the status of each effort is.

What

Projects within this call investigate solutions for a maintainable and responsive Internet. Some potential approaches to address this call are listed below:

- ### Realistic transition mechanisms

  Realistic transition mechanisms are a key aspect of any proposed technology upgrade – a perfect technology that cannot be deployed in practical terms will not be of much use. While satisfying all other design criteria, the following aspects need to be taken into account for any candidate alternative technology as early as possible: a) Research and develop feasibility of transition mechanisms b) Benchmark candidate alternative architectures with regards to scalability and efficiency, and the ability to isolate and contain the impact of legacy technologies on the new technology

- ### Provide real-time measurement data on Internet control plane

  Our understanding of issues with unintentionally antagonistic (legacy) devices such as middleware and customer premises equipment (CPE) directly impacts the feasibility of the introduction of the Next Generation Internet technologies. In order to analyse the health of the internet as a system, real-time and longitudinal measurement data is essential. These insights may help to improve limited upgrade capabilities by measuring and understanding the receptiveness of the deployed (legacy) infrastructure to systemic behaviour change.

- ### Improve emergency responsiveness by improving upgrade capabilities

  Currently there is limited capability to respond to network emergencies. Measures should be developed to improve upgrade capabilities and measures to isolate broken components or

undesirable behaviour. This could potentially include out-of-band countermeasures such as replacing or turning off specific broken or compromised components.

- Improve network equipment upgrade capabilities by removing obstacles

  A key research topic is how to isolate and circumvent the issues in network equipment, in order to increase the receptiveness of the overall system to new technologies being introduced. Some characteristics of legacy devices that need to be dealt with: Packet interference and rewriting due to missing or faulty support for modern protocols, NAT, lack of IPv6 support, firewall configuration errors and translation issues across protocols. Adoption can also be hindered by issues with connections: traffic shaping (including potential violations of net neutrality) and traffic loss issues due to for instance physical damage.

  - Develop best practices for solution deployability and maintainability
  - Improve deployability through pre-competitive bundling
  - Improve deployability and maintainability through reproducible solution integration
  - Collective management of updates and changes
  - Countering maintenance negligence

  Dealing with negligence with regards to maintenance should be recognised as a threat to the whole ecosystem. Create mechanisms to isolate known insecure systems that cause significant harm to others.

- Provide generic secure distribution of software/scripts and policies

  For the sake of consumers secure distribution and updating of software/scripts and policies should not depend on hard-coded internet addresses, as these easily break. Investigate complementary approaches, such as the possibility for signed updates to firmware, software and scripts to be provisioned through secure channels which are not linked to any particular owner.

3.11. Optimisable, extensible, reusable and reliable hardware

Specific challenge

Creating a future proof Internet infrastructure requires continuous optimisation and integration of best practises at all levels, including at the hardware and system integration level. Where the software market has been commodified and democratised through free software (aka open source), the hardware market is still dominated by a small amount of vendors. Commodification of networking and networked hardware (going from full-blown optical networking equipment to embedded systems and hardware cryptographic components) can help to ensure higher availability, lower costs, increase transparency and diversity, and create a more open market where anyone may introduce highly complex new services that require strongly optimised and well-integrated hardware and software. A better understanding and management of firmware is required as well.

Benefits

- Lower costs for market entrants
- Increased reusability of efforts
- Reduce market dominance of (mostly non-European) hardware vendors
- Increase transparency: complete understanding
- Increase market efficiency
- Improve energy use and resource efficiency

Communities/problem owners

- OEMs
- OpenPower, RISC-V Foundation,
- Semi-conductor industry (a.o. SEMI)
- Open Source Hardware Association
- OSADL, LibreCores, FOSSI
- Electronic circuit verification and logic simulation community
- CERN, ESA, ESFRI
- ACM SIGARCH

Resource planning

Phasing 

Required effort 

NGI Drivers for change

Resilience / Reliability		(5/5)
Transparency/ Trustworthiness		(5/5)
Sustainability/ Openness		(4/5)
Creativity and human potential enabler (user centricity,...)		(3/5)
Number of drivers impacted: 4	Overall impact on change:	18

Type of efforts and policy aspects

Research effort	✓
Development effort	✓
Maintenance and QA	✓
Standardisation effort	✓
Requires new policy measures	No
Significant educational effort required	-
Existing policy subject impacted	08 Competition policy 12 Energy 13 Industrial policy and internal market 15 Environment, consumers and health protection 16 Science, information, education and culture 18 Common Foreign and Security Policy 19 Area of freedom, security and justice Digital Agenda

Type of Action:

Research and Innovation Action (RIA)

Risks of not addressing this topic

- Loss of agency within NGI due to dependency on hardware vendors
- Inability to deal with overarching issues without market buy in
- Vendor specific feature delivery with low reusability
- Lack of responsiveness and lower efficiency in fixing issues due to wrong market incentives.
- Suboptimal development of ecological optimisations
- Opaqueness of hardware/firmware can lead to security breaches
- Inadequate capacity building and development of expertise leads to diminished competitiveness

What

Projects within this call are dedicated to open hardware and lower level software such as firmware. Proprietary hardware lacks transparency and trustworthiness, and puts artificial (legal) limits on the innovation power of the community - as well as illogical financial and legal barriers that block new technologies and new business models. The inability to modify aspects of the hardware and/or firmware also prevents power users from being able to assume full responsibility for their own security and safety in situations where this is urgently required.

Open hardware allows anyone to incrementally contribute new ideas to create the technologies necessary for the Next Generation Internet, and allows for verification and extension. The ability to optimise energy usage and create modular systems allows for replacing only select components, and as such is strongly connected to the topic of “greening”.

We need reusable open hardware primitives that can be optimised for in software, as well as technologies to verify the robustness and security characteristics.

Some potential approaches to address this call are listed below:

- Routing and cryptographic hardware

  High performance hardware (and components) optimised for modern networking protocols and cryptography

- Open implementations of hardware management/Trusted Platform Modules

  Controller subsystems with a minimal attack surface and verifiable integrity

- Firmware analysis tooling / International Firmware database

  The ability to analyse and match the weaknesses of binary firmware across vendors.

- Baseband processor

  Open and verifiable implementations of baseband controllers

- Verifiable open FPGA toolchains
- Verifable modular open GPU/CPU cores

4. Recommendations for the NGI Programme

This section presents recommendations for optimising the NGI programme through specific selection criteria for the projects proposed and for the intermediaries which will be implementing the calls with external stakeholders. In the current funding mechanism, intermediaries play a decisive role: the quality of their approach (from outreach, selection and quality assurance to inter-project collaboration and deployment) scopes the overall outcome. Given the many interdependencies and required critical mass, some form of higher level coordination will need to be devised – many larger issues won't be solved on a topic by topic basis. The organisation of the NGI as a whole will need to be architected with this in mind.

The selection criteria for the choice of projects to be funded are primarily defined from a user's perspective: within the actual granting process (which is expected to take place through a sub-granting mechanism), we suggest that among alternatives, competing projects may be selected based on their support for the largest number of NGI drivers for change – to maximise and speed up the outcome for the end user. However, technical dependencies should be respected: the right actions in the wrong order will not yield the desired result, and may in fact achieve the opposite result.

4.1. Selection criteria for projects

It is recommended that all call should be open for submissions of different sizes, from a large research and development topic to a small and targeted one. Each project proposer gives the requested budget.

Research and development

- **Impact**: **Contribution to the Vision**

  Ability to express and prove how their research or development will impact the drivers for change, and which of the drivers.

  For calls with many drivers, the number of drivers impacted is more important than the depth of impact.

- **Technology choice:**

  The choice of the technology will have to be defended based on feasibility of maintenance and interoperability potential.

- **Effectiveness of the solution**:

  The proof will have to be practical.

  The tenderer will explain how to baseline "resilience" today, and how they will measure the effect of the deployment of the solution on this baseline.

- **Soundness: Efficiency of the solution**

  Explain how this solution would be deployed, and by whom (inside or outside of the consortium).

Targeted research

- **Ecosystem**

  Explain how this targeted research is part of the bigger picture (if it is a building block of a larger solution, an ecosystem). Describe the environment in detail to show knowledge of this ecosystem.

- **Dependencies and deployment**

  Describe the dependencies with other research efforts for reaching the highest impact possible.

Explain, in this big picture, how the solution can be realistically deployed, what are the characteristics built in the solution supporting this (open source license, documentation of code, user-friendly interface etc.)

- **Fail Fast criteria**

  Describe approach and criteria for identifying early when the proposed research topic is not delivering on any outcomes ("Fail Fast") and what the fall back options would be for other research.

4.2. Selection criteria for intermediaries

Selected applicants for the role of intermediary will:

- Demonstrate a **verifiable track record** of activities and engagement with key actors in relevant:
  - standardisation organisations
  - cybersecurity research
  - the open source community
- Provide a **light-weight** and confidential application procedure that is:
  - minimally burdensome to applicants,
  - while providing adequate insight into technical capabilities as well as the urgency, relevance and relative cost effectiveness of the projects proposed.
  - assures a very high level of privacy for applicants
- While delivering the ability to:
  - extract the **technical merit** of projects proposed,
  - subsequently work together with successful applicants in a **staged approach** to identify and amend missing or inadequate aspects of their proposals prior (and conditional) to the start of the project.

In addition, the intermediary will provide the following:

- A **structured approach** to consistently apply the Framework Secure Software[1] (or equivalent best practices in security assessment and secure software development) across all projects.
- Technical expertise and infrastructure for **robust software development practices** throughout all the projects it supports, with each reaching at least the silver level of the Core Infrastructure Initiative Best Practices Badge[2] and including:
  a) reproducible builds on at least two platforms
  b) continuous integration and interactive testing
  c) central tracking of dependencies (versions and CVE)
  d) semantic versioning
- **Legal expertise** and support in reviewing provenance of third party open source projects throughout their life cycle with SPDX, including code governance.
- **Training support** for creating and maintaining high quality Developer, Packager and User Documentation. This includes translation/internationalisation infrastructure, support and training.
- Accessibility/Universal design criteria, so that user interfaces created by all projects **comply with WCAG guidelines** and will be verified as such conditional to final approval
- An independent **ombudsman function** for complaints and for internal whistle-blowers.
- A mechanism to flag teams and team members whose projects fail to pass the **review** in the application procedure for future projects. Failure to adhere to minimal standards means they are no longer be eligible for future funding.

1 https://www.securesoftwarealliance.org/FrameworkSecureSoftware_v1.pdf

2 https://bestpractices.coreinfrastructure.org/

4.3. Recommended additional quality criteria for intermediaries

In addition to the minimal criteria established in 4.2, **excellent** applicants for the role of intermediary will provide one or more of the following:

- **Complementary threat modelling** by independent experts prior to the start of a project. For each realistic threat, adequate mitigation shall be put in place in the final project plan. Every mitigation must be verified through e.g. formal proofs, (automated) testing or (at least) manual reviews of code, configurations, designs and protocols. Intermediaries should be able to effectively engage third parties to provide necessary complementary efforts to projects and/or provide these themselves if such is hygienic.
- A "**responsible disclosure**" procedure across all projects throughout the life cycle of the research programme:
  - Act with urgency and necessary resources to resolve the issue
  - Respond to incoming security reports within three business days with an evaluation of the report and an expected resolution date
  - Handle reports with strict confidentiality and not pass on personal details to third parties without permission
  - Keep security researchers involved informed of the progress on resolving the problem
  - After a major security issue has been solved, publish a report on its website explaining the vulnerability discovered and the measures taken to fix it
  - At the discretion of the security researcher, credit her or him as the person that first reported the vulnerability
- A complementary **external review** by an independent and knowledgeable party prior to final approval. A recommended minimum of 25% of overall project budget should be conditional to passing this external review on minimal software quality and security.
- A **bug bounty programme** across all projects for two years after the research programme has ended.
- A **public mirror** of all the repositories and source packages
- Compliance to the 2016 (or later) version of the **IEEE Code of Ethics**, or equivalent.

4.4. Overall recommendations on organising the NGI initiative

The rationale behind the selection of the three topics in chapter 2 over other topics that came forward during this process is how they fit in the overall intervention logic of the NGI. Such a logic is essential to impact the global internet where all efforts so far over the course of decades have run aground. The NGI should be considered to be a "**moonshot plus**" effort, both in effort and importance. The internet is the largest technological construct ever devised, and upgrading its technology and services to a next generation while continuing to carry the weight of the global economy and billions of critical users will probably the single largest collaborative effort in the history of technology.

Like the famous technology race to put the first person on the moon, the NGI will require an enormous amount of coordination, very careful engineering at different levels of technology, rigid quality assurance and solid integration. Clearly, the scale of this operation requires a long term vision – and to be honest, a lot of persistence, adequate mechanisms to commit the right human talent, political stamina and even a streak of luck. The viability and effectiveness of the NGI programme however primarily depends on its own design and execution: it shall create the conditions for its own success.

The unique promise of the Next Generation Internet initiative is its ability to leap into the future. NGI has the potential to transform today's internet into the internet we expected in the first place. An internet that is itself robust and safe to use without giving it a thought, efficiently scales to meet our collective needs, allows for diversity and growth, and reflects our core values. The NGI should develop the actual technology and tools that deliver (and not just mimic or allude to) those requirements – as well as the mechanisms and knowledge how these technologies and tools may be introduced in an internet that is itself fully operational. The latter would almost be a topic in itself, if it were not impossible to separate the two.

The first generation internet was not created to serve the needs of a global society, but to create remote access for the users of expensive computer equipment in the context of academic research under contract by the US military. Military contractors and institutions such as BBN, SRI and MITRE, played an important role in that period. There is much we do not know about how certain technologies really came into being, and we are unlikely to ever know. Yet it is certain that the internet is here to stay, and that we need the NGI initiative to fix and modernise it.

Use of the first generation of internet has reached into every realm of human activity, and with a limited set of legacy technologies was already able to empower completely different usage from doctors, factory owners and school children. The NGI will make important new additions to those capabilities, as well as restore the balance of power. The new logic of the internet aims to establish a new digital reality, with new ground rules that are more human-centric, fair and reliable. The vastly improvements in the overall characteristics of the new system are the key aspect the NGI initiative is aiming for.

The Next Generation Internet will not come about by itself. The very concrete bundles of technologies it will consist of will need to work together in an orchestrated and reliable way.

Without oversight, coordination and planning beyond short term projects, the risk is the NGI results once more in the creation of a 'cargo cult'-like mimicry of technology development. Given the urgency of the NGI vision, clearly that cannot be the desired outcome.

In the remainder of this chapter we will highlight a number of organisational aspects that will make or break the *intervention logic* of the NGI.

4.5. Getting organised as a precondition: maintainability by design

It is essential to make it easy for all future R&D efforts with the NGI Initiative to be widely **deployed** and **maintained**. For the NGI initiative to shape the next generation of the internet, the technologies it will sow and mature, will need to become ubiquitously used in the context of the actual internet environment. Even with the availability of iterative best practises and bundling of expertise, the cumulative cost of manual setup and maintenance of non-trivial new technologies has proven prohibitive to a large part of the internet population. This means slow uptake which in turn has led to large scale technical debt. The NGI initiative will introduce even more technologies, potentially impacting existing operations and requiring significant technical expertise. This means that there is little chance of succeeding without a converged, reliable path to deployment. In order to scale such deployment needs to be automated – through reproducible solution integration, pre-competitive bundling and automated testing and monitoring that the deployed situation is behaving as was intended. Keeping the internet safe, secure and up-to-date has asymmetric benefits and costs. The cost for maintenance has to be dealt with at the system level as an integral part of the process. The management of high volumes of updates/changes can only efficiently handled in a collective manner, and will fail when relayed to each individual participant.

4.6. Increasing responsiveness as an important secondary effect

The NGI Initiative needs to take many different challenges and opportunities into account, in the short term and in the long term. We require the technology stack of the future internet to be more responsive to changing environments and varying conditions, particularly in times of emergency. Major security issues like the Kaminsky DNS finding, and more recently SPECTRE, Meltdown and Nethammer have shown that almost overnight commodity technologies can turn into a major attack vector. We need to be able to (securely) upgrade the security baseline itself – not over the course of decades as technology is phased out slowly over time, but almost instantly. The technical community should have the capability to coordinate updates and take appropriate measures in the event of catastrophic system failure, degradation of performance, change in workload, or conditions of crisis, etc.

This improved responsiveness is in a way a by-product of the self-organising principles of the NGI initiative we recommend. The work to transform today's internet into its improved future self will be undertaken by many different individuals and teams. Each of them will be designing and developing solutions in parallel, within a limited scope. Each will be working with different parameters and with a large diversity of approaches. A major challenge for the NGI is to orchestrate at a higher level how to bring so many disjunct efforts together, and how to debug the overall system when it fails somewhere. The technologies created within NGI should work as expected in the real world, in every possible sane combination. As we are aiming to change the very technology fabric of the overall network itself, continuous changes to core technologies are assumed to be a given. As new technologies change behaviour one needs to take into account the impact on the other 'layers' of technologies – and vice versa for changes on that end.

Orchestrated intervention at internet scale requires oversight and systemic understanding, as well as convergence. The amount of parameters and continuously evolving complexity of multilateral efforts in the internet is already impossible for humans to track today. The way internet-related standards are maintained inside the IETF, W3C and other organisations is only a very limited reflection of the actual situation involving billions of old and new devices interacting real-time. Protocols, data formats and programming/binary interfaces are typically published in a traditional manner, as lengthy series of text documents that refer to each other. There is an unpredictable relationship between the offline reality of these technical specifications and the fragmented and often not-entirely-compliant technology deployed online. This has actually been one of the major roadblocks for healthy evolution of the internet so far, and must be dealt with at the start of the NGI.

Orchestrated intervention also requires significant and sustained investment above the project level. The technical timelines are expected to continue for a decade or more. The political and economic stakes are immense, and the interests of Europe most certainly collide with other interests. The NGI has no hidden agenda, other than to restore the balance of power at a global scale. This means there is potential broad support among the wider international community, but even in an optimistic scenario there are additional non-trivial challenges integrating into the complex global operational, economic and policy environment.

The way the NGI is architected and orchestrated at the highest level will be a deciding factor for its success. Better alignment across the various efforts and a well-thought out overall design will increase the viability of the NGI. It will also result in (much) lower maintenance and operational cost for future generations and higher efficiency of the resulting system.

4.7. Reliable and scalable shared procedures

The NGI effort as a whole should be manageable over the life cycle of the intervention. This requires the application of a number of basic shared procedures and the application of best practices at the level of each project:

- consistency and context-agnosticism in packaging and delivery so every result can be instantly used at NGI scale (such as source-based reproducible builds with proper distributed versioning) for all future NGI sub projects.
- continuous integration and automation of interoperability and regression testing (at the level of individual projects, across operating systems and throughout the entire internet technology stack as developed elsewhere within NGI)
- consistent issue and solution tracking and a shared bi-directional knowledge base across and beyond the NGI ecosystem (especially at the intersection of different proposed technologies, and the collision of existing and candidate technologies)
- use of secure upgrading and policy distribution mechanisms
- establishment and streamlining of best practices such as quality assurance mechanisms that may be applied transversally for the NGI to become a success.

There are a number of non-traditional, rather practical, efforts which will have to be made within or on behalf of each of the subprojects established within the NGI initiative. The NGI is assuming the responsibility for creating a trustworthy and working internet. The NGI initiative in full operation will be similar to a huge puzzle of technologies with new pieces being tried and tested all the time. Not every piece on the drawing table may work out in the end as expected or hoped for, but enough pieces will have to fit together for the whole NGI initiative to succeed in creating a next generation internet. This will for sure require mutual availability and outside exposure and testing during active development – and not afterwards when development teams may have been partially disassembled. Pending collisions between different projects should be made visible as early as possible. A precondition for any NGI subproject by any team should be that they are social, solid and reproducible: their technical status is transparent and results are always directly available as usable building blocks to all other projects within the NGI, across all layers.

There is need for a number of technical facilities and processes to help create convergence and oversight. Within the NGI initiative every actor should be able to discover and contribute all relevant issues, in particular outside of their own project scope. It would be unwise to confine these coordinating facilities exclusively to projects within the NGI initiative. While it is a major initiative that shall create a number of valuable new technical primitives, another (and just as important) role is to act as a catalyst for the wider technical internet community outside of the NGI initiative. The NGI as a real Next Generation internet can only succeed if Europe not only assumes but deserves global leadership in the larger international effort to upgrade the internet for the third millennium.

Annexe 1: Glossary

Communities and organisations

Note that we identify (pan-)European actors and stakeholders where available; many of the organisations have global reach, and/or actively work together with their counterparts across the world. This should by no means be seen as an exhaustive list.

Acronym	Description
ACM	Association of Computing Machinery
ACM SIGARCH	ACM's Special Interest Group on Computer Architecture
April	Association of free software advocates
CENTR	Council of European National Top-level domain Registries
CERN	European Organization for Nuclear Research
DHPA	Dutch Hosting Provider Associations
DINL	Digital Infrastructure Netherlands, association of large infrastructure stakeholders
ECO	Association of Internet Companies
EDRi	European Digital Rights, association of digital rights organisations
ENISA	European Union Agency for Network and Information Security
ESA	European Space Agency
ETNO	European Telecommunications Network Operators, association of telco's
EuroISPA	European association of internet service providers
EURO-IX	European Association of internet exchanges
FOSSi	Free and Open Source Silicon Foundation
FSF	Free Software Foundation
FSFE	Free Software Foundation Europe
GÉANT	Trans-European Research and Education Networking Association
GS1	Global Standards One, organisation behind barcodes and other standards related to distribution
IETF	Internet Engineering Task Force, publishes technical specifications of many core internet technologies
IFIP	International Federation for Information Processing
Internet Society	Global NGO promoting internet development
IRTF	Internet Research Task Force, performs longer term research into core internet technologies

MITRE corporation	American publicly funded private organisation that currently maintains a.o. the Common Vulnerabilities and Exposures (CVE) system
OpenCores	Commercially supported open hardware community
OpenPower Foundation	Consortium that supports the OpenPower Architecture
OWASP	Open Web Application Security Project
RIPE	Réseaux IP Européens, Community around technical development of the Internet
RIPE NCC	Réseaux IP Européens Network Coordination Centre, the Regional Internet Registry (RIR)
RISC-V Foundation	Foundation stewarding the open hardware Risc-V open instruction set architecture
W3C	World Wide Web Consortium, the Web standards organisation

Terminology

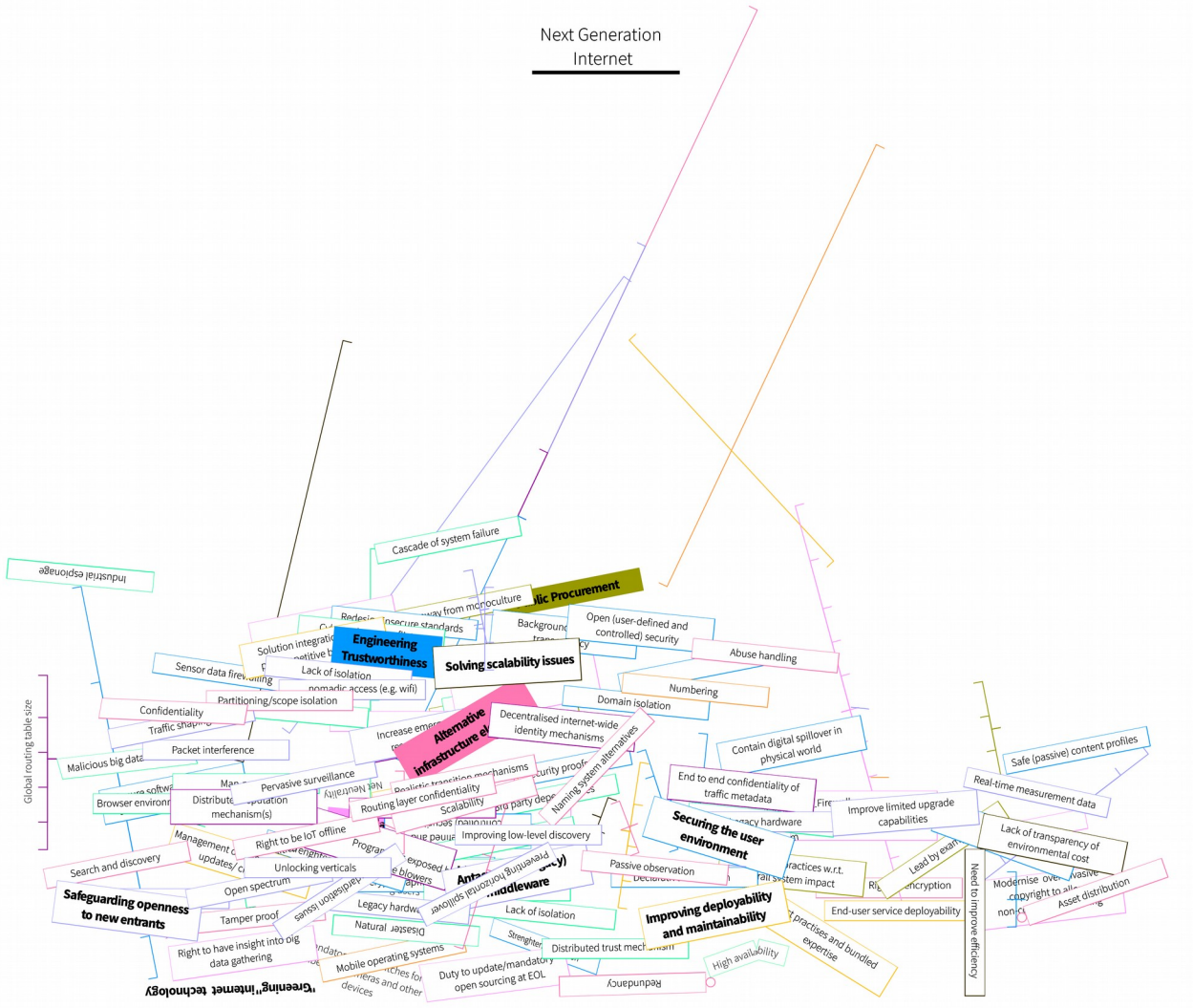
Term	Explanation
Binary analysis	Automated analysis of computer programs to search for potential security issues.
Browser vendors	Organisations that maintain web browsers (e.g. Mozilla, Google, Microsoft, Apple, KDE, Opera, Gnome, Palemoon) for desktop, mobile and embedded systems
CERT	Computer Emergency Response Team.
CMS	Content Management System.
Computer science	Scientific research into areas such as markup languages, cryptography, declarative interaction.
CPE	Customer-Premises Equipment, end-user middleware device located at a home or office
Cryptography	The field of computer science that researches techniques for securing (meta)data.
DNS operators	Organisations that run either authoritative (and to a lesser extent) recursive name servers
Formal proof	Applying formal logic to automate inference of the completeness of e.g. a protocol or piece of software.
Kernel teams	The teams that maintain the core (kernel) code for operating system runtimes such as Linux, Minix, FreeBSD, OpenBSD, Illuminos, MirageOS, etc.
Markup	Language syntax that encodes additional (machine readable) structure within documents
OEM	Original Equipment Manufacturers, e.g. people that make devices.
Static analysis	Automated analysis of computer source code to search for potential security issues.
UI	User Interface, the components of the software that deal with providing input and output to end users and other applications and devices.
UX	"User Xperience", e.g. the art of optimising the subjective experience of UI.

Annexe 2: EC Policy areas

This annexe lists the current official policy area categories as listed in EUR-lex.

	Policy area
1	General, financial and institutional matters
2	Customs Union and free movement of goods
3	Agriculture
4	Fisheries
5	Freedom of movement for workers and social policy
6	Right of establishment and freedom to provide services
7	Transport policy
8	Competition policy
9	Taxation
10	Economic and monetary policy and free movement of capital
11	External relations
12	Energy
13	Industrial policy and internal market
14	Regional policy and coordination of structural instruments
15	Environment, consumers and health protection
16	Science, information, education and culture
17	Law relating to undertakings
18	Common Foreign and Security Policy
19	Area of freedom, security and justice
20	People's Europe
	Digital Agenda

Source: EU Legislation: http://eur-lex.europa.eu/browse/directories/legislation.html


Next Generation Internet
Cascade of system failure
Industrial espionage
Engineering Trustworthiness
Solving scalability issues
Alternative infrastructure el
Decentralised internet-wide identity mechanisms
Open (user-defined and controlled) security
Abuse handling
Numbering
Domain isolation
Partitioning/scope isolation
Lack of isolation
Sensor data fire
Confidentiality
Packet interference
Malicious big data
Pervasive surveillance
Routing layer confidentiality
Scalability
Naming system alternatives
Contain digital spillover in physical world
End to end confidentiality of traffic metadata
Improve limited upgrade capabilities
Safe (passive) content profiles
Real-time measurement data
Lack of transparency of environmental cost
Global routing table size
Right to be IoT offline
Improving low-level discovery
Securing the user environment
Search and discovery
Unlocking verticals
Passive observation
Open spectrum
Tamper proof
Safeguarding openness to new entrants
Legacy hardware
Lack of isolation
Improving deployability and maintainability
End-user service deployability
Need to improve efficiency
Right to have insight into data gathering
Mobile operating systems
Duty to update/mandatory open sourcing at EOL
Distributed trust mech
Redundancy
High availability
"Greening" internet technology

Getting in touch with the EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact

On the phone or by email

Europe Direct is a service that answers your questions about the European Union.

You can contact this service:

– by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),

– at the following standard number: +32 22999696 or

– by email via: https://europa.eu/european-union/contact

Finding information about the EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union

EU publications

You can download or order free and priced EU publications at: https://publications.europa.eu

Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact).

EU law and related documents

For access to legal information from the EU, including all EU law since 1952 in all the official language versions, go to EUR-Lex at: https://eur-lex.europa.eu

Open data from the EU

The EU Open Data Portal (https://data.europa.eu/euodp) provides access to datasets from the EU. Data can be downloaded and reused for free, for both commercial and non-commercial purposes.

KK-02-18-778-EN-N

ISBN 978-92-79-86466-7
doi:10.2759/49503