Grant Agreement No.: 732569
Call: H2020-ICT-2016-2017
Topic: ICT-13-2016
Type of action: CSA

HUB4NGI

# D2.3 NGI GUIDE V3

| | |
|---|---|
| Work package | WP 2 |
| Task | Tasks 2.1, 2.2, with inputs from WP1, WP3 and WP4 |
| Due date | 31/12/2018 |
| Submission date | 28/01/2019 |
| Deliverable lead | IT Innovation |
| Version | 1.2 |
| Authors | Steve Taylor, Brian Pickering, Paul Grace, Michael Boniface (IT Innovation) Giulia Carosella, Richard Stevens, Andrea Siviero (IDC), Peter Van Daele (IMEC), Aba-Sah Dadzie (Open University), Claire Doble, Monique Calisti (Martel) |
| Reviewers | PSNC, Martel |


| | |
|---|---|
| Abstract | This document aims to assist the EC's NGI programme in transitioning the Internet to the NGI objective of a human-centric Internet. To address this objective, values have been determined that support human rights; challenges and threats that impede or violate these values have been identified; and addressing these challenges form the basis of recommendations for research, innovation and policy to support the NGI programme. |


| | |
|---|---|
| Keywords | NGI, Next Generation Internet, Values, Recommendations, Objectives, Goals, Roadmap, Evidence |

## DISCLAIMER



## COPYRIGHT NOTICE



| | | |
|---|---|---|
| Project co-funded by the European Commission in the H2020 Programme | | |
| Nature of the deliverable: | **R** | |
| Dissemination Level | | |
| PU | Public, fully open, e.g. web | ✓ |
| CL | Classified, information as referred to in Commission Decision 2001/844/EC | |
| CO | Confidential to HUB4NGI project and Commission Services | |

* R: Document, report (excluding the periodic and final reports)

DEM: Demonstrator, pilot, prototype, plan designs

DEC: Websites, patents filing, press & media actions, videos, etc.

OTHER: Software, technical diagram, etc.



Co-funded by the Horizon 2020 Framework Programme of the European Union

# SUMMARY: NGI VALUES, RECOMMENDATIONS & ROADMAP

As has been seen over the last quarter-century, the Internet is a social revolution and has had huge benefits. It is also a huge social experiment that is still ongoing, and civilisation is finding its way through the mass of opportunities, issues and threats that the immediate and ubiquitous communication the Internet offers.

This document aims to assist the EC's NGI programme in transitioning the Internet to the NGI objective of a human-centric Internet. To address this objective, values have been determined that support human rights; challenges and threats that impede or violate these values have been identified; and addressing these challenges form the basis of recommendations for research, innovation and policy to support the NGI programme.

## NGI VALUES

In keeping with the EC's stated goal of a human-centric Internet, values have been derived from analysis of the Internet's impact on human rights, specifically the rights described in the Universal Declaration of Human Rights[1]. In addition, the NGI Vision comprises three pillars – *Resilient*, *Trustworthy*, *Sustainable* – and these also served as a point of departure for establishing the values. The values are founded within the protection of rights and freedoms and determine high-level aspirational principles that can guide the NGI development, the stakeholders who develop the NGI and the actors who use it. The values are deliberately aspirational: it will be impossible to address any of them completely, but they provide worthwhile high-human-centric objectives that define a clear direction of travel for development of the NGI.

### Trustworthiness

The Internet must be trustworthy, meaning that a user must be able to make a judgement about the risks involved in using the Internet, and decide that the risk is acceptable.

### Safety & Resilience

The Internet must be safe to use. The user must not be hurt by using it and protected from threats and exploitation. The Internet is now a critical infrastructure, depended on by people worldwide, so its infrastructure should also be robust and resilient to attacks and threats.

### Truthfulness & Transparency

Biased content and deliberate misinformation should be minimised, and citizens need to be educated to identify so-called "fake news". Transparency for the processing of Internet users' data and the provenance of information delivered via the Internet should be emphasised as priorities and mechanisms to enable them should be supported.

### Fairness & Sustainability

The Internet should support equal and fair opportunities for all users of all types. The Internet should also provide sustainable opportunities for human employment, incentivise economically sustainable business models and promote environmentally-sustainable technology.

## RECOMMENDATIONS FOR RESEARCH AND INNOVATION

Recommendations have been determined in key thematic areas, to address the challenges and threats that impede the progress towards a human-centric Internet. They are briefly described

[1] The analysis is provided in Appendix 1 in Section 6.1



Co-funded by the Horizon 2020 Framework Programme of the European Union

below and are summarised in roadmap form in Figure 1, organised into the key themes and colour-coded to indicate which of the NGI values each recommendation addresses. Detailed recommendations, with timescales and justification, can be found in Section 3.2 of the main body of the document.

- ***Trustworthiness as an Overarching Framework:*** ensuring a trustworthy Internet (in its many forms) is critical to users retaining faith in it; and other areas of recommendation can all contribute to this.
- ***Data Sovereignty:*** Internet users need visibility and control over their data when processed in the Internet.
- ***Decentralisation & Democratisation:*** supporting democratisation by investigating and promoting decentralised, open and fair data sharing ecosystems; and addressing risks of Internet monopolies.
- ***Flexible & Agile Workforces:*** investigating how to educate a highly adaptable human workforce resilient to quickly-changing employment demands.
- ***Supporting Informed Opinions:*** to understand and address the Internet's contribution to opinion manipulation caused by misinformation, polarisation and confirmation bias.
- ***Safe Internet & Resilient Infrastructure:*** to continue to address the many and varied threats to Internet users, and to address the weaknesses in the current Internet stack.
- ***Ethical AI:*** to address concerns regarding responsibility and ethical issues surrounding AI & autonomous systems, and their impact on society.
- ***Free Speech & Liberty in the Digital Age:*** to understand how the Internet affects balances between national security, personal safety and the rights and freedoms of citizens.

## POLICY RECOMMENDATIONS FOR IMPLEMENTATION & MANAGEMENT OF THE NGI PROGRAMME

Policy recommendations for implementation and management of the NGI programme have been determined from experiences in HUB4NGI. They are listed below and summarised in Figure 2. Detailed recommendations are found in Section 3.3 of this document's main body.

- ***Multidisciplinary Collaboration, User Participation & Community Building:*** to ensure that technological developments are (at least) legal, ethical and socially acceptable, support for multidisciplinary collaboration and co-creation involving Internet users is strongly advocated.
- ***Innovation Support:*** help innovators test & evaluate their developments at scale in realistic conditions and bridge the so-called "innovation gap" between research results and innovative products and services that are commercially marketed.
- ***Technology Support:*** continue to support research and innovation in key technology areas identified by the community, whilst scanning the horizon for new useful technologies.
- ***Sustainable Development:*** incentivise sustainable innovation through dedicated actions, policies and innovation programmes.



Co-funded by the Horizon 2020
Framework Programme of the European Union

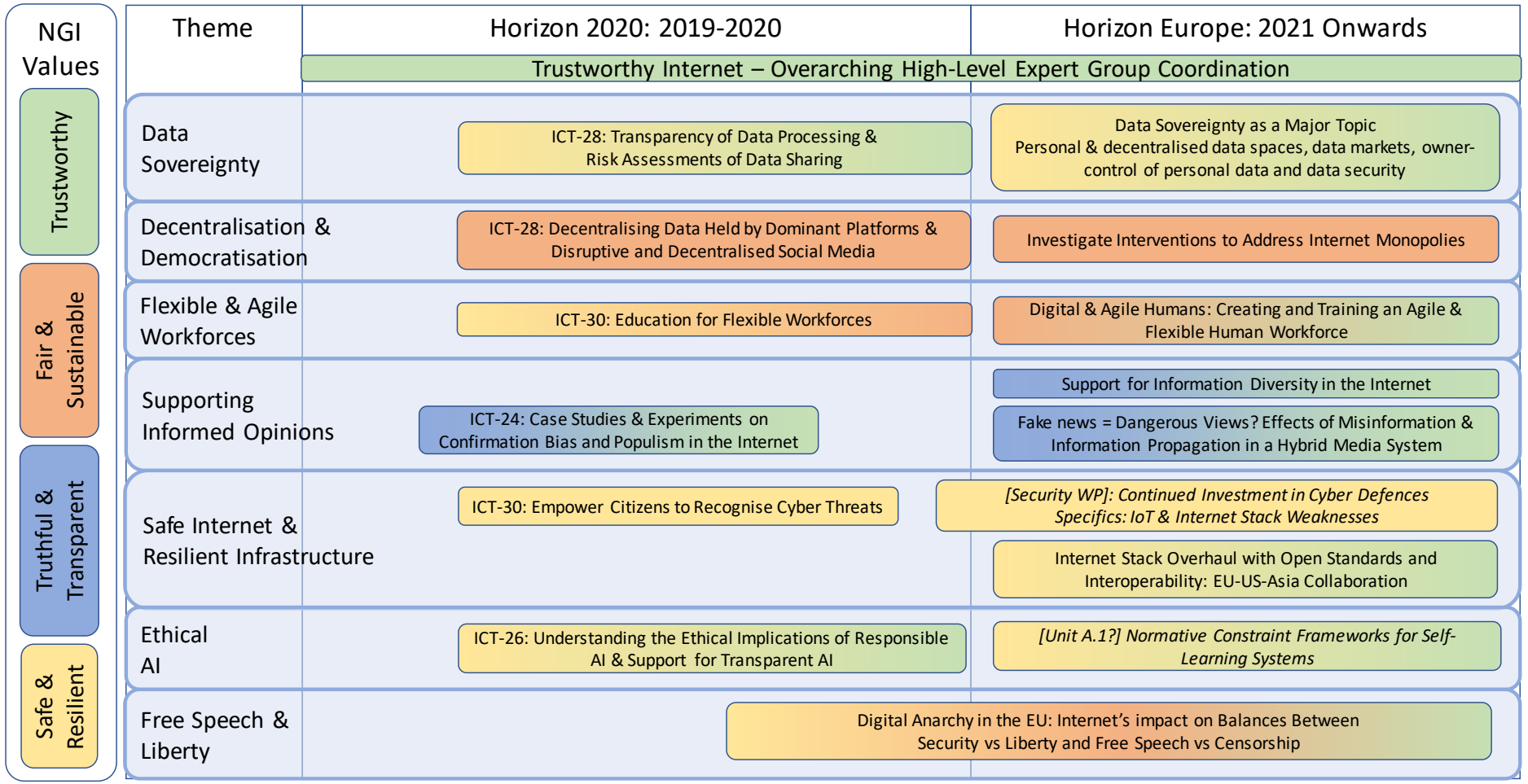


FIGURE 1: ROADMAP FOR RESEARCH AND INNOVATION IN THE NGI

Figure 1 shows the roadmap of recommendations for research and innovation in the NGI. The NGI Values are shown at the left and the recommendations in the roadmap are colour-coded to indicate the values they contribute to. Many recommendations contribute to more than one value, and this is indicated by their multi-colour shading. The Roadmap is divided into thematic areas (horizontal groups), and in time: 2019-2020 (H2020) and 2021 onwards (Horizon Europe).





Co-funded by the Horizon 2020 Framework Programme of the European Union

| Theme | Horizon 2020: 2019-2020 | Horizon Europe: 2021 Onwards |
|---|---|---|
| Multidisciplinary Collaboration & Community Support | Support Multidisciplinary Collaboration: Networking Events, Participation Portals, Innovation Hubs, Funding Conditions | |
| | Continue Supporting the NGI Community Cascade Funding Projects Building Communities, Events, Online Directories | |
| Innovation Support | Support NGI initiatives to translate research results into commercial products and services: Collaboration Events, Marketing Support, Cross-National Support | |
| | Provide shared infrastructures, tools and data to support innovation: Validation of ideas, Scalability Testing, Help innovators their turn their proofs of concept into market ready products | |
| | Open Call & Open Access Enhancements Fast-Turnaround SME Calls, Open Access with Funded Support | |
| | Explore Other Types of Cascade Funding e.g. Case Studies, Reference Data Sets, Specific Surveys & Questionnaires, All Kinds of Experiments | |
| Technology Support | Support research and innovation in key technology areas identified by the community | |
| | Continue to support innovation using established technologies | |
| | Keep funding horizon scanning projects | |
| Sustainable Development | Continue to incentivise sustainable innovation through dedicated actions, policies and innovation programmes | |

FIGURE 2: KEY NGI POLICY & SUPPORT RECOMMENDATIONS

Figure 2 shows the key policy recommendations for implementation of the NGI programme and support of the NGI community, grouped horizontally into thematic areas. These recommendations are not time-dependent, rather they are ongoing, and ideally should start as soon as possible, so they are shown as across the remainder of H2020 and into Horizon Europe.





Co-funded by the Horizon 2020 Framework Programme of the European Union

# TABLE OF CONTENTS





Co-funded by the Horizon 2020
Framework Programme of the European Union

# LIST OF FIGURES





Co-funded by the Horizon 2020
Framework Programme of the European Union

# ABBREVIATIONS

| | |
|---|---|
| **AI** | Artificial Intelligence |
| **AR** | Augmented Reality |
| **EC** | European Commission |
| **ELSE** | Economic, legal, socioeconomic |
| **FAANG** | Facebook, Amazon, Apple, Netflix, Google |
| **GAFA** | Google, Amazon, Facebook, Apple |
| **GDPR** | General Data Protection Regulation |
| **IoT** | Internet of Things |
| **IP** | Internet Protocol |
| **NGI** | Next Generation Internet |
| **OECD** | Organisation for Economic Co-operation and Development |
| **ORD** | Open Research Data |
| **RAM** | Responsible Autonomous Machines |
| **SDN** | Software Defined Networking |
| **TCP** | Transmission Control Protocol |
| **UDHR** | Universal Declaration of Human Rights |
| **VR** | Virtual Reality |



Co-funded by the Horizon 2020
Framework Programme of the European Union

# 1 INTRODUCTION

This deliverable is a summary of recommendations from the perspective of the HUB4NGI CSA, cast into the form of a roadmap that is intended as input to the processes that determine the upcoming work programme for the Next Generation Internet. The recommendations cover two major themes:

- research and innovation needed to address the major challenges of the Next Generation Internet; and
- policy recommendations for implementation and management of the NGI programme to enable and support the NGI community of researchers, innovators and experimenters.

The key guiding principle is that the Next Generation Internet be human-centric. The methodology adopted in this deliverable has taken this principle to heart, and as a result this deliverable has determined human-centric values for the NGI that protect human rights and freedoms, which are presented in the roadmap as aspirational goals for the NGI. Even though Internet benefits many people, it hosts many threats and challenges that threaten and impede the human-centric values set out as goals of the NGI. These threats and challenges have been identified, and from them, research and innovation requirements are determined to address them and clear the way to achieving the NGI's goal of a human-centric Internet. To determine actual recommendations for research and innovation, the research and innovation requirements have been compared against the current NGI work programme as a gap analysis. The identified gaps form the basis of this deliverable's recommendations.

This deliverable presents the perspective of the HUB4NGI CSA and is based on the studies it has conducted. This deliverable is in no way intended to be the definitive sum-total of the recommendations to the EC in the determination of the upcoming NGI work programme. This deliverable is explicitly intended to be one of several inputs to the consultation process that determines upcoming work programmes, each representing a different perspective. The primary purpose of this deliverable is to provide credible, justifiable and actionable recommendations that are clearly based on evidence, rather than attempt to be exhaustive.

This deliverable is focused on addressing societal challenges and how they contribute to a human-centric Internet. There are other technology-themed work programmes, but the NGI is general in its focus. Therefore, this deliverable's focus is explicitly not on recommending technologies: it is asserted that the best technology for addressing a challenge should be the choice of a researcher or innovator, and they should be free to choose the best technology and justify that choice, unfettered by technology choices prescribed by the work programme.

In addition, this document provides an overview of the guiding principles and main research and innovation directions for the Next Generation Internet framework in Horizon Europe [22], which extends its focus beyond the current NGI Unit/scope to embrace advanced smart infrastructures, services and enablers – see Section 4.

The structure of this deliverable is as follows. The methodology is described next, followed by the roadmap in the form of the NGI human-centric values and recommendations for research, innovation and community support, followed by indications on future directions for NGI Horizon Europe and brief conclusions. The evidence and analysis work supporting the derivation of the values, threats, challenges, gap analysis and community support are provided as appendices and referred to in the main text where necessary.



Co-funded by the Horizon 2020
Framework Programme of the European Union

# 2 METHODOLOGY

The key objective for this deliverable is to suggest practical, actionable and justifiable recommendations for research & innovation and implementation of the NGI work programme that supports the goal of a human-centric Internet for the remainder of H2020 and into Horizon Europe. To this end the methodology shown in Figure 3 has been followed.

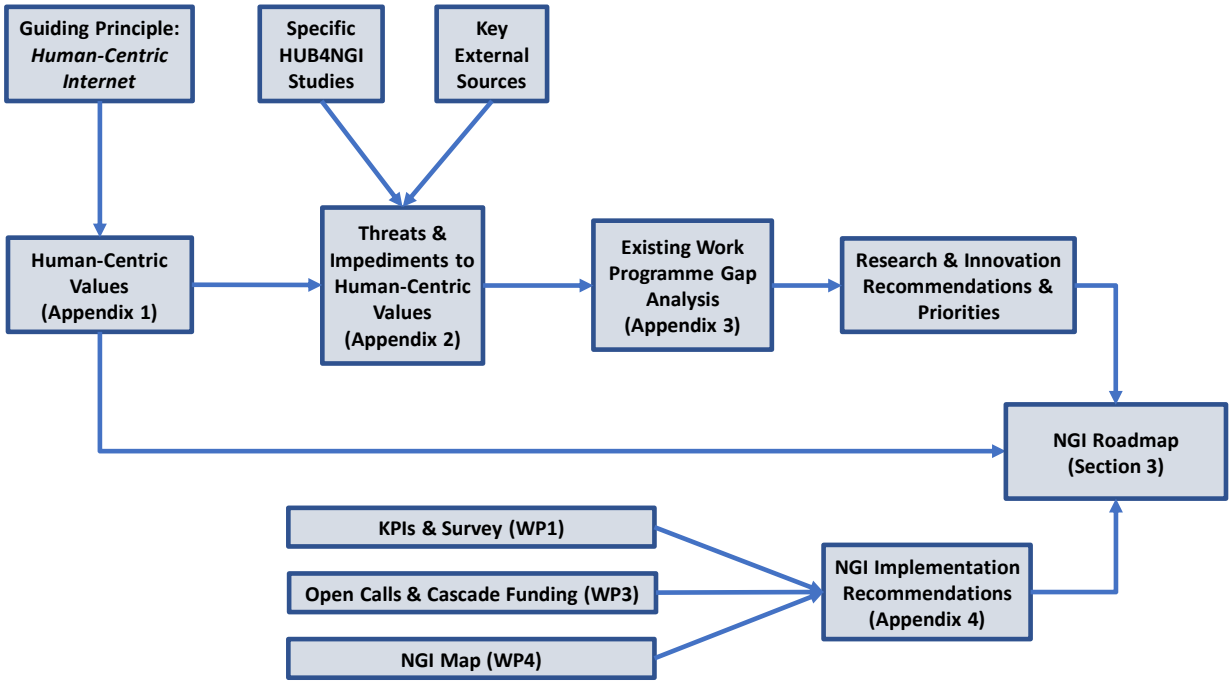


FIGURE 3: HUB4NGI D2.3 METHODOLOGY

Given that the EC's stated aim of the NGI is a human-centric Internet, the starting point for the methodology was to determine key values that the Internet and its users should aspire to. These values have been derived from an analysis of the Internet's impact on the Universal Declaration of Human Rights (UDHR), as described in Appendix 1 (Section 6.1). The values themselves are presented at the start of the Roadmap (Section 3.1).

Following the determination of human-centric values, impediments, threats and challenges preventing the achievement of the goals represented in the values were identified. HUB4NGI work and key external sources have been examined to determine a set of threats and challenges to human freedoms and rights that the Internet poses, and the output of this analysis is a set of requirements for research and innovation in the NGI to address the challenges and support the values. The analysis work for these challenges is described in Appendix 2 (Section 6.2).

Once the requirements for research and innovation have been determined, a gap analysis of the current NGI work programme was undertaken to determine where the research innovation requirements were already addressed, where they were not addressed, and where they needed expanding or augmenting. The analysis describing the gap analysis is presented in Appendix 3 (Section 6.3), and its result comprises the actual recommendations for research and innovation, which are presented in the Roadmap.

In parallel to the analysis of research and innovation requirements, Recommendations for the implement of the NGI programme, especially in support of the NGI community, have been derived from the work done in HUB4NGI WPs1-4, and reported in other deliverables (the most current of which are D1.3, D3.2 and D4.4). The recommendations from this are fed into the Roadmap as suggestions for NGI community support and implementation of the NGI programme and include experiences of running cascade funding open calls (WP3), KPIs to measure the success of the programme and the results of a survey of NGI participants (WP1), plus the organisation of community-building events in WP4.



Co-funded by the Horizon 2020 Framework Programme of the European Union

The Roadmap presented in Section 3 is structured to follow the organisation of the methodology. First, the human-centric NGI values derived from the UDHR are presented as aspirational goals, then the recommendations for research and innovation priorities derived from the challenges and impediments to the goals are presented in terms of suggestions for near-, medium- and long-term research objectives, short-duration and longitudinal work. Finally, suggestions for implementing the NGI work programme and concluding with general suggestions and observations.



Co-funded by the Horizon 2020
Framework Programme of the European Union

# 3 FUTURE DIRECTIONS FOR THE NGI

This section contains the roadmap towards the NGI. It leads with objectives expressed as human-centric values, then recommends research and innovation topics to address, prioritised for H2020 and Horizon Europe in terms of timing, but also highlighting smaller and larger topics. Policy recommendations for implementing the NGI based on experiences from HUB4NGI are also covered.

## 3.1 NGI VALUES SUPPORTING HUMAN RIGHTS & FREEDOMS TO ACHIEVE A HUMAN CENTRIC INTERNET

The NGI Values described in this section are founded within the protection of rights and freedoms for all individuals. They are derived from analysis of the Internet's impact on human rights as described in the Universal Declaration of Human Rights (described in Appendix 1 (Section 6.1). The values determine high-level aspirational objectives that can guide the NGI development, the stakeholders who develop the NGI and the actors who use it. The values are deliberately aspirational: it will be impossible to address any of them completely, but they provide worthwhile human-centric objectives that define a clear direction of travel for development of the NGI.

### *3.1.1 Trustworthiness*

The Internet must be trustworthy, meaning that a user must be able to make a judgement about the risks involved in using the Internet, and decide that the risk is acceptable. While clearly people use the Internet in vast numbers, there is a growing trend of mistrust in the motivations of other users, powerful corporations and governments, as well as in the truth of the content held within Internet servers. There must be enough evidence in general circulation that enables an average citizen to feel comfortable using the Internet. Contributors to trustworthiness include evidence of the following.

- Transparency & accountability, especially of personal information processing, e.g. what information is stored, what is done with it and by whom.
- Visible countering of untruths & fake news, e.g. fact checking or reputation of news sources.
- Protection of the user from attacks, e.g. widely available security and malware protection toolkits, plus regulation designed to provide protection from harm with associated penalties for transgressors.
- Fairness & equal opportunities, e.g. addressing imbalances of power and providing equal chances for all users to gain benefit from the Internet.

### *3.1.2 Safety & Resilience*

The Internet must be safe to use. The user must not be hurt by using it and protected from threats and exploitation. The threats are many and varied, and include cyber-attacks, privacy violations including identity theft, personal information leaks, surveillance, malware & ransomware, cyber fraud and offensive, obscene or hateful content.

### 3.1.3 Truthfulness & Transparency

Biased content and deliberate misinformation should be minimised as much as possible. The Internet is highly influential, due to its status as a mass media channel of varying content, some of which is professionally created and some of which is user-generated. It is very difficult to avoid opinions being influenced by Internet content, but it is a worthwhile objective to aim to prevent



Co-funded by the Horizon 2020 Framework Programme of the European Union

the perversion of opinions via biased Internet content, deliberate misinformation or propaganda, which can lead to polarisation, ignorance, intolerance and extremism.

Transparency for the processing of Internet users' data and the provenance of information delivered via the Internet should be emphasised as priorities and mechanisms to enable them should be supported. It is currently unclear what happens to Internet users' data once they submit it to e.g. platforms due to opacity and obfuscation. In addition, many users do not know that the content they are seeing can be biased, for example the search results they get may be tuned based on profiling of their behaviour, and consequently they may never be aware that different viewpoints exist.

### 3.1.4 Fairness & Sustainability

The Internet should support equal and fair opportunities for all users of all types. Imbalances of power are currently prevalent, with a few large corporations providing most of the services used within the Internet and the opportunities for alternatives are limited.

The Internet should also provide sustainable opportunities for human employment rather than reduce them: automation threatens employment, so it is an objective to seek a balanced and flexible economy to accommodate the needs of human workers whist still retaining the efficiencies of automation.

## 3.2 RECOMMENDATIONS FOR NGI RESEARCH AND INNOVATION

One of the key challenges for the HUB4NGI consortium has been identifying strategic directions for a completely new initiative (rather vaguely defined especially in the first period its life) that according to its ambition gathers potentially many and quite diverse research and innovation areas. To re-invent the Internet, means to be able to redesign and transform many aspects at different levels, from more physical/networking foundation, to data processing aspects, to privacy, to interactive/multimedia technologies, to AI and any more or less autonomous learning and reasoning algorithmic aspects, to socio-economic mechanisms and business models, etc. Given that many of these aspects appeared later (after NGI first 6 months) to be of more direct concern to other research areas, the focus, as also recommended by the NGI EC representatives, has been on identifying challenges and thereby priorities more specifically related to create a more human-centric Internet.

Therefore, this section contains key recommendations for NGI research and innovation that describe the recommended work to support the human-centric NGI Values and address threats to them, grouped into broad themes (reflected in the subsection headings below). The recommendations are predominantly socio-economic by nature, but with technical implications, and this reflects the human-centric guiding principle of the NGI, as well as the societal impact of the Internet and the threats to humans using it. The Next Generation of the Internet needs to serve humanity, so therefore the issues to be tackled are by nature multidisciplinary, involving as much soft science as technological development. Each recommendation is in a standardised format that describes the Title, Objective, Specific action, the timescale (H2020 or Horizon Europe mainly), and the justification, which includes references to earlier sections where the need for the work is highlighted, and the Values that the work contributes to.

### 3.2.1 Trustworthiness as an Overarching Framework

| Title | Trustworthiness as an Overarching Framework |
|---|---|
| Objective | To coordinate the many different threads that contribute to a trustworthy Internet. |
| Action | It is recommended that trustworthiness in the Internet be adopted as an overarching theme, into which research into many different themes can be |



Co-funded by the Horizon 2020 Framework Programme of the European Union

| | |
|---|---|
| | marshalled. To implement this, it is recommended that a high-level expert group be founded with the remit of enhancing Internet trustworthiness with a high-level strategic overview, comprising experts in multiple disciplines (e.g. politics, sociology, economics, cyber security, privacy, data protection, networking etc). This group can assess the factors that contribute and detract from public trust in the Internet from their multiple perspectives and provide guidance to steer the research as necessary to support the contributors or address the detractors. This guidance could be suggesting synergistic collaborations between research efforts, recommendations for new research, or suggestions for new directions for existing research, for example.<br><br>The factors currently identified in this work include the following, but it is expected that public trust in the Internet will evolve as new issues and threats emerge, so the assessment of trustworthiness and the factors that influence it will need to evolve to keep pace.<br><br>• Transparency & accountability. Investigation is needed into how transparency and accountability can be supported. This will include technical factors, such as exposure of e.g. monitoring information or processing chains, but will also require related socio-economic investigation, for example the interests of the parties involved – how can they be incentivised to provide transparent processing?<br><br>• Cyber security. An ongoing effort involving monitoring of threats and determination of countermeasures to address the ever-evolving threats is clearly needed.<br><br>• Data security. Ensuring that data held is not vulnerable to leak, theft or corruption, and providing credible assurances to the owners of the data that the data is secure.<br><br>• Robustness and resilience of the infrastructure, so that it is not prone to failure and resistant to attacks.<br><br>• Guarantees of privacy support & respect. Investigation is needed into how privacy protection can be supported, and personal data protected, as well as providing enforceable guarantees to citizens, all in an easy to understand and transparent way. An assessment is also needed regarding the provisions of the GDPR in terms of how they can be practically implemented, and whether there are gaps that need to be filled.<br><br>• Information quality & accuracy. Citizens need mechanisms to help them determine the validity of information they find in the Internet. |
| Timescale | Should start soon (2019) but be long-lived. |
| Justification | It is a priority to understand the full spectrum of trustworthiness in the Internet – identifying factors that contribute to trustworthiness and those that detract from it, so that the contributors can be supported, and the detractors can be addressed.<br><br>The theme of "trust" is a vast, multifaceted subject that has been discussed in Section 6.2.1, where it is asserted that public trust is declining in the Internet, so there is a need to marshal the different aspects to understand how addressing them can contribute to an increase in the trustworthiness of the Internet. Indeed, any perceived threat has significant potential to reduce levels of trust, so most of Section 6.2 is relevant to the theme of trustworthiness in the Internet. Specific examples include Section 6.2.4 |



Co-funded by the Horizon 2020 Framework Programme of the European Union

| | |
|---|---|
| | concerning the specific case of trustworthy AI and Section 6.2.9 covering the manipulation of citizens' opinions using (amongst others) Internet channels.<br><br>Therefore, the theme of trust cuts across many other subjects and requires multiple strands of coordinated and in-depth research to address the challenge sufficiently. Some of this work can be within the NGI, but others (in particular cyber security) are covered in other focus areas, so it is likely that coordination across these focus areas will be necessary.<br><br>This recommendation contributes to the *Safety* and *Trustworthiness* Values. |

### 3.2.2 Data Sovereignty

Internet users feel powerless regarding what is being done with their data. Clearly the owners of data need to be in control of it, wherever it is being stored or processed. There are already efforts in personal data spaces, i.e. enabling users to be in control when sharing data, and data portability, avoiding lock-in to a particular provider or platform, but other aspects need to be investigated to complement this work, and the work organised into an overarching theme to coordinate it.

| Title | Data Sovereignty as a Major Horizon Europe NGI Topic |
|---|---|
| Objective | To adequately address the issues surrounding data sovereignty. |
| Action | Data Sovereignty should be a major topic in the NGI upcoming work programmes, funding significant RIA projects covering aspects including personal & decentralised data spaces, data markets, owner-control of personal data and data security. CSA projects can coordinate, enable collaboration and investigate new directions. |
| Timescale | NGI-2019 to Horizon Europe. This is a major topic, so needs long-term support. |
| Justification | Data sovereignty, i.e. owner-control of personal data and full control over data sharing is mentioned in multiple subsections of the ICT-24 topic, within "Privacy and Trust Enhancing Technologies", "Decentralised Data Governance" and "Service and data portability". These are small, short-term innovation projects, and the issues surrounding these topics need further in-depth research. Given that data sovereignty is a major theme that concerns the users of the Internet, for example privacy violations contribute to a decline of trust in the Internet (discussed in Section 3.1.1), and also compromise personal freedoms and rights (discussed in Section 3.1.6), it is suggested that data sovereignty have a topic in its own right.<br><br>This recommendation supports the UDHR Article 12 - the Right to Privacy and Reputation (Section 6.1.1) and Article 17 – the Right to Property and Protection from Theft (Section 6.1.2) through enabling the closer control of personal data.<br><br>This recommendation contributes to the *Safety* and *Trustworthiness* Values. |

| Title | Techniques to Enable Transparency and Accountability of Personal Data Processing |
|---|---|
| Objective | To enable owners of personal data to understand quickly, easily and accurately where their data is, who is processing it, and how it is being processed. |



Co-funded by the Horizon 2020 Framework Programme of the European Union

| | |
|---|---|
| Action | Extend ICT-28 to include a specific RIA call dedicated to enabling transparency & accountability of processing of personal data, including audit trails of data processing and guarantees of conformance to users' wishes (for example guarantees of non-transmission, data security, data integrity and permanent deletion) with appropriate penalties for non-conformance. |
| Timescale | NGI 2020. |
| Justification | Privacy abuses contribute to a decline of trust in the Internet (discussed in Section 3.1.1), and also violate personal freedoms and rights (discussed in Section 3.1.6), so it is clear that users need transparency and guarantees on how it is processed at third parties.<br><br>As discussed in Section 6.3.5, ICT-28 has an Innovation Action covering business models, governance and proofs-of-concept for secure and fair sharing of data, but transparency of processing and guarantees for data owners are not included.<br><br>This recommendation supports the UDHR Article 12 - the Right to Privacy and Reputation (Section 6.1.1) and Article 17 – the Right to Property and Protection from Theft (Section 6.1.2) through enabling the more transparent and accountable processing of personal data.<br><br>This recommendation contributes to the *Safety* and *Trustworthiness* Values. |

| Title | Techniques to Enable Risk Assessments of Personal Data Sharing |
|---|---|
| Objective | To enable owners of personal data to make judgements on the risks of sharing personal data with third parties. |
| Action | Extend ICT-28 to include a specific RIA call dedicated to investigating the vested interests of different stakeholders in a personal data sharing ecosystem, the risks to them, the mitigation strategies that they can employ, and how these affect other stakeholders. Investigations should produce decision support tools for data owners to help them make informed choices regarding sharing their personal data. |
| Timescale | NGI 2020. |
| Justification | As discussed in Section 6.3.5, ICT-28 has an Innovation Action covering business models, governance and proofs-of-concept for secure and fair sharing of data. A key aspect that is missing is examination of the vested interests of the parties and how this affects the risk levels of the owner of the data.<br><br>This recommendation supports the UDHR Article 12 - the Right to Privacy and Reputation (Section 6.1.1) and Article 17 – the Right to Property and Protection from Theft (Section 6.1.2) through enabling better informed judgements about the sharing of personal data.<br><br>This recommendation contributes to the *Safety* and *Trustworthiness* Values. |

### 3.2.3 Decentralisation & Democratisation

This section concerns decentralisation and democratisation in two major forms: the decentralisation of personal data to give users greater control, and decentralisation of the monopolistic power currently held by few dominant incumbent corporations in the Internet.



Co-funded by the Horizon 2020 Framework Programme of the European Union

Connected with the previous theme of controlled data sharing, there is a theme of decentralising data, which augments the work already identified in data portability.

| Title | Decentralising Data Held by Dominant Platforms |
|---|---|
| Objective | To find ways to bring in the dominant and monolithic (e.g. social media) platforms that hold vast quantities of personal user data into decentralised open and fair data sharing ecosystems. |
| Action | Extend ICT-28 to include a specific IA call dedicated to investigating how the dominant incumbent platforms that hold vast quantities of personal user data can be encouraged to participate in more open data sharing ecosystem, where the users are empowered to control the processing on their own data. |
| Timescale | NGI 2020. |
| Justification | As discussed in Section 6.3.5, ICT-28 has an Innovation Action covering business models, governance and proofs-of-concept for secure and fair sharing of data. A key aspect not mentioned that should be considered is how these models and structures affect the dominant platforms, who are likely to see no reason to move to new models, and so investigations into how to incentivise the dominant platforms into participating in these models is needed.<br><br>If the outcome of this recommendation is successful and dominant platforms participate in fair data sharing ecosystems, this recommendation supports the UDHR Article 12 - the Right to Privacy and Reputation (Section 6.1.1) via more transparent and accountable processing of the personal data they hold.<br><br>This recommendation contributes to the *Equal Access & Opportunities* Value. |

| Title | Disruptive and Decentralised Social Media |
|---|---|
| Objective | To understand how new kinds of social media (e.g. distributed and peer to peer) can compete with the dominant platforms that have a critical advantage in that they already hold vast quantities of personal user data. |
| Action | Extend ICT-28 to include a specific IA call dedicated to investigating how new kinds of social media (already funded as RIA projects in ICT-28) can be made competitive to the existing incumbent and dominant platforms.<br><br>If results from these studies are positive, IA projects in Horizon Europe can investigate and implement scaling up of these disruptive and decentralised social media platforms. |
| Timescale | Early studies in NGI 2020, leading to Horizon Europe. |
| Justification | As discussed in Section 6.3.5, ICT-28 contains one Research and Innovation Action covering investigations into decentralised and distributed social networks, as an alternative to the current monolithic incumbent platforms. As with the previous comment, there is a need to investigate how these new architectures will affect the current incumbents, but also how users can be encouraged to migrate to these new social network architectures, especially when the dominance of the current incumbents is founded upon a critical mass that they have already achieved. How can any new entrants compete?<br><br>This recommendation contributes to the *Equal Access & Opportunities* Value. |



Co-funded by the Horizon 2020 Framework Programme of the European Union

There is a rising fear of monopolies, in that most peoples' interactions with the Internet are via a small number of dominant corporate entities, e.g. search engines or social media platforms. Research is therefore needed to investigate the impact of advancing automation, on the employment landscape and to assess and mitigate the risks of monopolistic situations. humans may be sustained in the event of mass redundancy through automation.

| Title | Creating a Europe-led Decentralised Internet Supporting Equality and Fairness |
|---|---|
| Objective | To understand how to address the risks associated with monopolies of large, dominant, incumbent corporations controlling major portions of the Internet. |
| Action | In the Horizon Europe work programme, support large-scale multidisciplinary investigations into monopolistic situations from a socioeconomic risk- and inequality- analysis perspective, to understand the risks and inequalities, together with strategies for addressing the risks and inequalities, using, for example regulation, data owner in control and transparency. The work should also assess existing strategies employed to address monopolies – what is different in the Internet economy? A specific inequality aspect that should be investigated is the implication of user lock-in on large platforms, plus how it may be addressed, e.g. using data portability, or alternative social media structures, as discussed in Section 6.3.5, so lessons can be learned from the results of ICT-28. There are also cross-overs here with the Data Sovereignty recommendation, so lessons can be learned from outputs of work already funded in ICT-24 and if the recommendation for Data Sovereignty as a major theme in Horizon Europe are taken up, this topic can run alongside it and they can learn from each other's results (a CSA could coordinate the results from the two streams of work). This work has global implications and should involve perspectives from different global regions, so intercontinental collaboration (with e.g. US & Asia) on this subject would be very beneficial. |
| Timescale | Horizon Europe. |
| Justification | Section 6.2.7 covers the dominance of large incumbent corporations, and discusses the need for investigations concerning the implications of monopolistic economies delivered over the Internet (for example the impact of platforms), the risks and inequalities these monopolies pose, and how the risks and inequalities may be addressed.<br><br>This recommendation contributes to the *Equal Access & Opportunities* Value. |

### 3.2.4 Flexible & Agile Workforces

There is a fear that automation will threaten employment and new, flexible economies are needed to address this threat. There is already a division of labour between humans and machines, but this is likely to evolve as the machines become more sophisticated and become able to perform more sophisticated tasks. A key objective is for human labour to be a highly flexible, agile and adaptable resource, and human training needs to evolve with automated systems' capabilities to address the areas where humans are needed.

| Title | Digital & Agile Humans: Creating and Training an Agile & Flexible Human Workforce that Embraces Digital Developments and AI |
|---|---|
| Objective | To understand how to educate a human workforce so that it is adaptable to ever-changing human employment requirements caused by advances in technology and automation. |



Co-funded by the Horizon 2020 Framework Programme of the European Union

| | |
|---|---|
| Action | Foster a collaborative approach to incorporating digital education & training, digital ethics and human needs to train an agile workforce of tomorrow / (using the internet of tomorrow)<br><br>This is a large subject, and must involve multidisciplinary teams working together, for example psychology, sociology, pedagogy, economics as well as technology.<br><br>First steps to address this topic can be to extend ICT-30 to cover investigations into educational programmes that can enable citizens to adapt to changing employment requirements over their working lifetimes. ICT-30 investigations are likely to be preliminary studies, so it is recommended that this topic carry on in Horizon Europe.<br><br>To understand the risks of automation & AI to human employment and to determine the requirements for a situation where humans and automated systems can both be adequately and harmoniously sustained, it is suggested to have a call in Horizon Europe regarding the impacts of automation & AI on human employment. For example, to determine what characterises AI and how is it different from previous automation revolutions? Factors could be self-learning and adaptation, potential for pervasive disruption across multiple industries simultaneously (speed & scope of disruption). How will these affect the employment market? Understand the human / machine split at present. Determine key trends for change in automation (with justification) e.g. over next 10 years. This research is necessarily multidisciplinary, as it involves at least technology, sociology and economics. It may consider new employment opportunities created because of the automation (for example design, maintenance and adaptation) but equally may consider future wealth distribution models where full human employment is no longer an objective of a successful economy.<br><br>It is an open question as to which part of the work programme this topic can be best placed – it could easily fit within NGI but equally other parts (concerning education or Unit *A.1 "Robotics & Artificial Intelligence"* for example), so this is left for discussion. |
| Timescale | NGI 2020, leading into more in depth studies in Horizon Europe. |
| Justification | Section 6.2.8 is dedicated to specific threats to employment.<br><br>Section 6.2.4 concurs with this threat, but specifically from AI systems: AI's impact on human workers needs to be investigated – how any threats or negative effects such as redundancy or deskilling can be addressed.<br><br>Section 6.3.3 identifies a gap in the current ICT-26 AI platform call - investigation of the socioeconomic impacts of AI & autonomous machines on society, especially how AI automation differs from other types of disruptive mechanisation.<br><br>Section 6.3.7 identifies a need (referring to Section 6.2.8) for understanding how to educate a workforce of citizens so that it is sufficiently adaptable to changing employment needs is needed.<br><br>AI is a current focus for employment threats. There have been numerous cases of disruptive technological advances throughout history, and typically after a short-term shock, humanity has adapted and returned to prosperity. The key difference with AI as an automation technology is that previous technologies have been deterministic, designed to accomplish a specific task, |



Co-funded by the Horizon 2020 Framework Programme of the European Union

| | |
|---|---|
| | whereas if the predictions of Artificial General Intelligence[2] come to pass, AI will be self-learning and adapting, meaning that an AI system will learn from its environment to enable itself and its spawn to accomplish new tasks. AI can duplicate itself immediately and anything learned in an AI system is instantly reproducible, as opposed to humans who need time and effort to mature and learn new skills. Current research indicates that AI technology is a long way from AGI currently: what is currently seen as AI is narrow, highly specialised smart tools, but the threat to human unemployment is increasing with each advance, so it is important to understand the social and economic consequences of non-deterministic self-learning and self-replicating technologies.<br><br>This recommendation directly supports the UDHR Article 23 - the Right to Employment (Section 6.1.5) and indirectly supports Article 26 – the Right to Education (Section 6.1.6) via its intention to use education to create a flexible workforce that is employable throughout its working life.<br><br>This recommendation contributes to the *Trustworthiness* and *Equal Access & Opportunities* Values. |

### 3.2.5 Supporting Informed Opinions

There is considerable risk that phenomena such as misinformation, propaganda, fake news and echo chambers undermine liberal democracy and the pursuit of enlightenment, so investigations are needed into how opinions are formed and manipulated in the current digital age**.** Therefore, it is suggested that there be a topic in the Horizon Europe NGI entitled *"Understanding and Addressing the Internet's Contribution to Opinion Manipulation, Polarisation and Confirmation Bias"*. This covers how people can be manipulated or have biases confirmed using the Internet.

| Title | Fake news = Dangerous Views? The Effects of Misinformation and Information Propagation in a Hybrid Media System |
|---|---|
| Objective | To understand how misinformation creation and propagation translates into measurable effects, and to understand how misinformation propagates in a hybrid media system that can incorporate online and offline transmission over broadcast and / or social media. |
| Action | Long-term (e.g. 10-year) studies are needed to understand the effects of misinformation transmitted over the Internet. Measurable effects (e.g. such as election results, increased in polarisation or extreme views) need to be identified, measurement criteria and hypotheses regarding the causal relationship from misinformation to them need to be tested, and it is expected that these will necessarily be long-term studies, so as to give time for the effects to manifest and to be measured. The effort for these studies may not be excessive, e.g. a medium-sized RIA, but the effort is spread over the long time-frame of the project.<br><br>It is also recommended to have a call in Horizon Europe NGI to study the propagation of misinformation, for example experiments to investigate how misinformation spreads online and offline and including techniques to join & correlate offline propagation with online. Studies should also aim to understand how misinformation is represented in broadcast and social media and when they interact – how does a social media post translate into broadcast media, and then do the comments on a broadcast story get into |

[2] An early example of the definition of AGI is in: Laird, J.E., Newell, A. and Rosenbloom, P.S., 1987. Soar: An architecture for general intelligence. Artificial intelligence, 33(1), pp.1-64.



Co-funded by the Horizon 2020 Framework Programme of the European Union

| | |
|---|---|
| | social media? Different types of media – e.g. blogs, traditional media with an online presence, online-only newspapers, polemics – how to determine reputations & trustworthiness of these? |
| Timescale | Long-term (e.g. 10-year) study beginning in Horizon Europe. |
| Justification | Section 6.2.9 reporting on the HUB4NGI "Opinion Forming" Consultation discusses the threats of misinformation and explicitly recommends understanding the societal effects of fake news – whether people believe it, whether and how they distribute it and whether they are influenced by it, and recommends determination of effective and observable measures for the influence of fake news. Investigations into the creation and spread of misinformation are needed, especially coupled with understanding of its tangible outcomes (for example whether it affects voting in elections). At the current time, it is suspected that fake news is highly impactful, but it is not clear what the concrete effect of spreading propagandist and sensational material aiming to manipulate opinions is, and how this effect is achieved.<br><br>This recommendation indirectly supports the UDHR Article 26 - the Right to Education (Section 6.1.6) via the intention to better understand the effects of misinformation, which can lead to more effective countermeasures, thus promoting truthfulness.<br><br>Section 6.2.9 also recommends that the propagation of fake news needs to be studied, especially within and across hybrid media systems, which can be any or all of: online, offline, broadcast and social media.<br><br>As discussed in Section 6.3.5, ICT-28 contains an Innovation Action covering content verification in social media, and this clearly crosses over with the fake news aspect of the Opinion Forming consultation. However, the Innovation Action covers just social media and a key recommendation of the Opinion Forming consultation is that misinformation propagates over a hybrid media system, with different kinds of media (online, offline, broadcast and social media) interacting as necessary, so there is a need for expanding the scope of the misinformation to include other media types.<br><br>This recommendation contributes to the *Trustworthiness* and *Truthfulness & Impartiality* Values. |

| Title | Case Studies and Experiments into Internet "Echo Chambers", Conformation Bias and the Internet's Contribution to Recruitment into Populist Movements |
|---|---|
| Objective | To understand from example case studies how confirmation bias manifests itself in Internet communities, that can be referred to as "echo chambers", and to understand from example case studies how the Internet's communication channels are mobilised to assist recruitment of citizens to populist movements. |
| Action | In the third phase of ICT-24, have a topic concerning the Internet's influence on confirmation bias and populist recruitment, with the cascade funding used to commission specific case studies or experiments. A specific point to address is to understand distinctions and interplay between confirmation bias and critical analysis – when do people choose to critically analyse or just accept information they receive over the Internet, and how do the channels contribute to the choice? A second specific point is to investigate how search engine filtration contributes to polarisation through the user not receiving a |



Co-funded by the Horizon 2020 Framework Programme of the European Union

| | |
|---|---|
| | balanced viewpoint. A third point, specifically suited to case studies, is the study of individual Internet communities that support polarised viewpoints.<br>• Case Studies: The result should be a library of published case reports with accompanying data from e.g. social or broadcast media on the Internet stored archivally as Open Research Data.<br>• Experiments: test hypotheses or use other research methods such as surveys or interviews regarding echo chamber or Internet-supported populist recruitment situations suggested by the case studies or from elsewhere, and publication of complete datasets gathered for the experiments should be mandated so as to aid further experimentation.<br>Cascade funding open calls can support these case studies, and the administering project can collate, analyse and synthesise the results of the case studies. |
| Timescale | NGI 2019-2020. |
| Justification | Section 6.2.9 discusses the need to characterise "echo chambers" and how they are manifested in the Internet. We need to understand how conformation biases are supported using the Internet communication channels, especially how the hybrid media system (including any of: online, offline, broadcast and social media) contributes. Research is also needed to determine distinctions and interplay between confirmation bias and critical analysis, and to investigate how search engine filtration contributes to polarisation.<br>Section 6.2.9 also discusses the need to understand how people are socialised into populist movements. The phenomenon of populism is well studied, but we specifically need to understand the contribution of hybrid media systems including interactive online communities, plus fake news and echo chambers' contributions to populist recruitment; individually and in conjunction.<br>The "Discovery and Identification Technologies" ICT-24 theme covers advanced search topics but does not cover the challenge of search engines filtering content based on profiling of Internet users.<br>This recommendation supports the UDHR Article 26 – the Right to Education (Section 6.1.6) through better understanding of the mechanisms that undermine truthfulness by promoting polarisation. This recommendation also directly supports the UDHR Article 21 – the Right to Democratic Government (Section 6.1.4) through better understanding of the mechanisms by which democracy can be undermined by populist movements.<br>This recommendation contributes to the *Trustworthiness* and *Truthfulness & Impartiality* Values. |

| Title | Investigations into How to Promote Information Diversity in the Internet |
|---|---|
| Objective | To understand how to present Internet users with "balanced" viewpoints. |
| Action | Have a call in Horizon Europe with the objective of determining tools, techniques and technologies that can provide a balanced viewpoint to Internet users. This can be via, for example, alternative search tools that are not subject to filtration, or specifically find opposing viewpoints, or alternative social media fora that promote diversities of viewpoints. Attention needs to be paid to how balanced information is presented, as presentation needs to be sensitively handled to avoid being off-putting to the user. |



Co-funded by the Horizon 2020 Framework Programme of the European Union

| | |
|---|---|
| Timescale | Horizon Europe, learning from case studies in H2020 NGI ICT-24 |
| Justification | Section 6.2.9 discusses the need for diversity in Internet content, so as to counteract polarisation, and Section 6.1.6 on Article 26 of the UDHR discusses the right to education, which clearly needs to be unbiased. Whilst it is a noble aim to work towards a truthful Internet, defining "truth" is difficult because it can be highly subjective. Bias is similarly difficult to define, as again it is subjective, but if users are not presented with a complete set of information and only see information that supports one side of an argument, polarisation and entrenched beliefs can result. To address these challenges, research is needed into providing a balance of viewpoints with Internet content. How this balance of viewpoints is delivered is also a subject for investigation, but a key guiding principle is that it needs to be unobtrusively and sensitively presented: in many cases people do not want to see opposing viewpoints to their own or to have their beliefs continually challenged, so investigations are needed into how any kind of attempt to de-bias information or present a balanced viewpoint can be presented sensitively to the user.<br><br>This recommendation supports the UDHR Article 26 – the Right to Education (Section 6.1.6) through promotion of balanced viewpoints.<br><br>This recommendation contributes to the *Trustworthiness* and *Truthfulness & Impartiality* Values. |

### 3.2.6 Safe Internet & Resilient Infrastructure

This section concerns cyber security and addressing the security vulnerabilities of the ageing Internet stack.

For cyber security, the recommendations mainly concern another area of the work programme, namely *14. Secure societies - Protecting freedom and security of Europe and its citizens,* so detailed recommendations will not be made because they out of the NGI's scope, but general principles and observations may be made, and are reported here. It is advocated that a close relationship is maintained between the organisers of the cyber security work programme and those organising the NGI, as there are clear cross-overs between the two, and that these recommendations may be transmitted from the NGI to the cyber security organisers. The general recommendations are as follows.

- The discussion in Section 6.2.2 clearly reinforces the need to continue investment in cyber security, because the attackers will not stand still, and so the defences need to keep pace: new threats will continually emerge, and constant vigilance to identify new threats is required. The penalty for defence advances falling behind the sophistication of the attacks will be severe to catastrophic.
- A joined up, worldwide collaborative approach is needed to address the challenges of cyber threats. The research needs to be conducted using multidisciplinary and multinational approaches, so as to capture the full breadth of the attack spectrum, and to accommodate any national or geographic differences.
- The current foci highlighted in Section 6.2.2 are defence against attacks on critical infrastructures (covered in SU-INFRA01), destabilisation of governance and political systems (covered in the counterterrorism topics SU-FCT01 to SU-FCT04 inclusive), investigating the threats and weaknesses of IoT devices (not covered) and addressing weaknesses in lower layers of the Internet (not covered), so if recommendations for the Secure Societies call are required, they would be to include investigations into IoT threats and to address the weaknesses of the lower layers of the Internet technology stack. For both areas, discussions would be required to determine where support for



Co-funded by the Horizon 2020 Framework Programme of the European Union

such work would be best located, as they could equally fit within cyber security or the NGI.

There is one specific recommendation directly relevant to the NGI, regarding education in ICT-30, discussed next.

| Title | Empower Citizens to Recognise Cyber Threats |
|---|---|
| Objective | To empower non-expert citizens to make informed judgements about the risks and threats of different locations in the Internet. |
| Action | Extend ICT-30 (or stipulate in its cascade funding calls) to include creation of educational programmes informing ordinary citizens how to understand the dangers of the Internet. |
| Timescale | NGI 2020. |
| Justification | One key challenge not mentioned in ICT-30 the need to understand how to provide education to enable Internet users to make informed judgements about the risks and threats of Internet locations and content (discussed in Section 6.2.2 within the context of cyber threats).<br>This recommendation contributes to the *Safety* and *Equal Access & Opportunities* Values. |

The Internet's infrastructure is at risk, because it relies on decades-old protocols and the Internet stack contains numerous weaknesses, each of which is vulnerable. Clearly the entire stack is necessary and contains many weak links, so addressing them is a priority to remove the weaknesses.

| Title | Internet Stack Overhaul with Open Standards and Interoperability: EU-US-Asia Collaboration |
|---|---|
| Objective | To enable addressing of the weaknesses in the current Internet stack, whilst providing backward compatibility with the existing stack and being fully open standardised. |
| Action | Include Internet Stack Renovation in Horizon Europe as a major theme, and agree with other world regions partnership programmes, to foster the collaboration necessary to agree the standard for such an undertaking.<br>It is possible that an overseeing mechanism for this could be a High-Level Expert Group (HLEG). This could undertake the steering of the work at the high level and be the primary contact point for inter-continental collaboration.<br>In shorter term, preparation for this collaboration in Internet Stack renovation would be a good candidate for EU-US collaboration. This can build bridges and prepare the ground for a larger scale collaboration in Horizon Europe. |
| Timescale | Long-term, large scale programme beginning early in Horizon Europe (2021). This programme may need to extend beyond Horizon Europe in time due to its complexity and the need for worldwide agreement, but it should begin in Horizon Europe. |
| Justification | Renovating the internet architecture addresses key threats identified in Section 3.1.2. As discussed in Section 6.3.1, there is currently an open call in ICT-24 for addressing this challenge, but small, close-to-market open calls are not adequate to address this challenge. Addressing these challenges will require a huge effort and collaboration on a global scale. Standardisation will be a key factor for interoperability and understanding, and an endeavour of this magnitude and fundamental nature needs to be open, multi-stakeholder |



Co-funded by the Horizon 2020 Framework Programme of the European Union

| | |
|---|---|
| | and multi-continental so as to avoid any partisan or proprietary commercial or national bias or advantage. In addition to determining new standards and re-engineering the Internet stack, enabling seamless transition from existing stack technologies is necessary so that there are no service interruptions.<br><br>This recommendation contributes to the *Safety* and *Trustworthiness* Values. |

### 3.2.7 Ethical Artificial Intelligence

As AI impinges on everyday life, especially when applied in safety critical situations, or in roles that can affect citizens' wellbeing, concerns are rising regarding responsibility and ethical issues surrounding these autonomous systems and their impact on society.

| Title | Understanding the Ethical Implications of Responsible AI |
|---|---|
| Objective | To understand ethical implications of different AI applications on society |
| Action | For the 2020 ICT26 call, it is suggested to provide for open calls to commission detailed ELSE-focused application case studies for AI, investigating the impact of the AI on the application case. The case studies should include relevant laws, failure modes, remedial actions, how the laws may not be adequate and how they can be augmented to allow for self-developing artificial intelligence. Responsibility issues also should be considered, i.e. what are the factors that determines who (or eventually what) is responsible in a situation and what characterises the situation. What are the obligations on the responsible party?<br><br>Lessons can also be learned from post-facto studies of AI transgression – e.g. previous cases of AI failures and what we can learn from them. ICT-26 cascade funding can also be used to commission post-facto case studies. |
| Timescale | 2020 ICT-26 Call |
| Justification | As discussed in Section 6.2.4, in order for AI systems to be trustworthy and accepted into society, the issues regarding responsibility, ethics, accountability, transparency etc will need to be addressed.<br><br>Section 6.2.4 also recommends Certification of "safe AI" and accompanying definitions of safety criteria, as well as determination of remedial actions for situations when AI systems malfunction or misbehave is recommended but investigation is needed into what existing remedial actions are appropriate in what situation and whether they need to be augmented. The application context determines the societal impact of an AI system so the safety criteria and resulting certification are likely to depend on the application the AI is put to. New applications of existing AI technology may need new assessment and certification.<br><br>Evaluating the current ICT-26 call, Section 6.3.3 identifies the need for case studies to investigate the implications of different AI application cases. The scope of the analysis in the case studies covers ELSE plus other aspects: it is advocated that ethical considerations; responsibility & accountability; relevant regulations & legislation; monitoring of behaviour; and failures & remediation are covered.<br><br>This recommendation contributes to the *Safety* and *Trustworthiness* Values. |

| Title | Support for Transparent AI in ICT-26 AI Platform |
|---|---|



Co-funded by the Horizon 2020 Framework Programme of the European Union

| | |
|---|---|
| Objective | To address the need for transparency in AI decision making. |
| Action | ICT-26 in 2020 should have dedicated aspects on AI transparency – how to achieve it in both training data and in decision making. It is suggested that the AI platform determine a methodology for creation and archiving of robust training sets with provenance information, and that the training datasets be made available as Open Research Data. The methodology will need to determine criteria such as what constitutes bias, provenance of source data, how it is annotated, outcomes as a result of the data. |
| Timescale | 2020 ICT-26 call |
| Justification | Section 6.2.4 advocates that in order for AI systems to be trustworthy and accepted into society, the issues regarding responsibility, ethics, accountability, transparency etc will need to be addressed.<br><br>Section 6.2.4 also recommends that AI decisions and actions need to be transparent, explained and justified; and the explanation needs to be comprehensible by lay people as AI systems become more exposed to the general public. It also recommends that provenance information regarding both AI decisions and their input data (as well as any training data) needs to be recorded in order to provide an audit trail for an AI decision.<br><br>Section 6.3.3, evaluating the gaps in the current ICT-26 AI platform call, identifies the need for AI transparency as a key objective of the AI platform. It is advocated that a library of training data, annotated with provenance information be built, which is publicly accessible to benefit other users apart from its creator.<br><br>This recommendation contributes to the *Safety* and *Trustworthiness* Values. |

| Title | Normative Constraint Frameworks for Self-Learning Systems |
|---|---|
| Objective | To support AI safety and trustworthiness by providing boundary constraints that allow self-learning systems to grow and improve, whilst remaining within acceptable limits. |
| Action | Investigations into how to provide constraint frameworks for self-learning systems, that can give the systems the freedom to self-improve but constrain their behaviour to acceptable norms are needed. From this, frameworks can be built to monitor behaviour and raise alarms for transgressions. It is recommended that RIA calls are included in the work programme to understand the normative constraints that apply, and once this is understood, further RIA calls are included to determine how to create normative governance and transgression frameworks. |
| Timescale | Horizon Europe expected. This is a major challenge so needs long-term funding. This may be beyond the scope of the NGI and may be more suited to Unit A.1: “Robotics & Artificial Intelligence” |
| Justification | Many AI systems are self-learning and improving, and this means that they are not deterministic, so it is difficult to regulate them. If, however, normative frameworks are created that allow these systems to improve and adapt to their environment, but only within acceptable constraints, so they do not cause harm.<br><br>Section 6.2.4 recommends Certification of “safe AI” and accompanying definitions of safety criteria are recommended. |



Co-funded by the Horizon 2020
Framework Programme of the European Union

| | |
|---|---|
| | This recommendation contributes to the *Safety* and *Trustworthiness* Values. |

### 3.2.8 Free Speech & Liberty in the Digital Age

Free speech and liberty need to be examined in the context of the digital age, to examine the contribution of the Internet to two perennial debates: *national security vs liberty* and *free speech vs censorship*.

| Title | Digital Anarchy in the EU: Investigate the Internet's impact on the Balances Between Security vs Liberty and Free Speech vs Censorship |
|---|---|
| Objective | To understand how the Internet affects the balance between national security, personal safety and the rights and freedoms of citizens. |
| Action | Have a call in H2020 to support investigations into the balances between national security and citizens' liberties, and the trade-off between free speech and control of information.<br><br>Key questions include: How do the communication channels of the Internet affect this debate, and what are the implications of liberty restrictions on citizens' communication via the Internet (e.g. surveillance or national censorship)? Under what circumstances is information control is legitimate, and when should free speech should prevail? Factors to be considered include differences in attitudes and social norms within different European countries, and how the norms can change over time or as a response to events (e.g. terrorist attacks).<br><br>This could be conducted as a CSA gathering information, surveys, and outlining local methods and initiatives from the NGI Contact Points. Where in the H2020 programme this should be supported is moot. It could be supported in the H2020 NGI programme, or *"13 Europe in a changing world – Inclusive, innovative and reflective societies"* equally programmes in other units (*"G.2: Interactive Technologies, Digital for Culture & Education"* for example), so discussions between the organisers are needed to determine the best fit. |
| Timescale | NGI 2020 |
| Justification | As discussed in Section 6.2.5 concerning limitations to personal freedoms and rights, governments trading personal freedoms for national security is not a new theme (and varies from country to country), but new sources of threats are via the Internet itself (e.g. cyber-attacks as discussed in Section 6.2.2), but the Internet is clearly a means of social utility that used properly can enhance freedom of expression. In a world of increased demands on national resources, accelerating cyber-attacks and ubiquitous connection to the Internet, there is a risk that personal freedoms enabled by the Internet especially are eroded (e.g. via censorship of Internet content or online surveillance) to address national security challenges. Investigations into the question of national security vs liberty with a special focus on the contribution of the Internet's channels and stakeholders need to be undertaken from a multidisciplinary legal, ethical and socio-economic (ELSE) perspective, especially considering violations of privacy (discussed in Section 6.1.1 on Article 12 of the UDHR concerning the right to privacy).<br><br>Also, as discussed in Section 6.2.5 on threats to personal freedoms, there is a tension between the protection of free speech, which clearly can contain misinformation, propaganda and extreme material; and censorship, which may be well-intentioned in aiming to protect citizens or be driven by political or state-control ends. At either end of the spectrum, the situation is likely to |



Co-funded by the Horizon 2020 Framework Programme of the European Union

| | |
|---|---|
| | be detrimental for citizens. The age-old debate between freedom of expression and censorship needs revisiting in the digital age, in the context of propagandists' deliberate manipulation of information and with the addition of the Internet as the communication channel. How do key features of the Internet e.g. speed of communication, access to vast amounts of (verified and unverified) information, interconnectedness of community etc influence this debate?<br><br>This recommendation addresses issues raised in the discussion of the UDHR Article 29 – Responsibility to the Community & Legitimate Limitations of Rights and Freedoms (Section 6.1.7) through examination of the balance between personal liberties and national security (the responsibility to the community). It also addresses issues discussed in Section 6.1.3 on Article 19 of the UDHR concerning the right to freedom of expression.<br><br>This recommendation contributes to the *Safety, Trustworthiness* and *Equal Access & Opportunities* Values. |

## 3.3 POLICY RECOMMENDATIONS FOR IMPLEMENTATION OF THE NGI PROGRAMME

This section contains recommendations for implementation of the NGI programme. They are often general recommendations based on the experiences gathered in HUB4NGI, so are not targeted at specific calls, and in many cases do not have timescales, but clearly the sooner they are implemented, the better.

### 3.3.1 Multidisciplinary Collaboration, User Participation & Community Building

| Title | Support and Promote Multidisciplinary Collaboration |
|---|---|
| Objective | To ensure that the technological developments are (at least) legal, ethical and socially acceptable. |
| Action | Support for multidisciplinary collaboration is strongly advocated. Almost all the external sources, survey respondent and consultees have mentioned this as a major enabling factor to a human-centric Internet. Mechanisms to encourage multidisciplinary collaboration can include the following.<br><br>• Conditions in funding calls for proposals requiring the applications to demonstrate multidisciplinary collaboration in their consortium.<br><br>• Organising events with a wide scope in their programming that attendees from different disciplines will find attractive (for example in collaboration with other parts of the H2020 work programme such as Security or Societies), and within these facilitate networking to enable the attendees to discover each other's capabilities.<br><br>• Promoting networks of innovation hubs and other tools (for example the NGI community map and search functionality) that can enable discoveries and introductions between multidisciplinary people.<br><br>• Involving the users is a fundamental part of this collaboration. To enable this, promote co-creation and agile development through initiatives such as participation portals. |
| Timescale | 2019 Onwards. Ongoing CSA – NGI4ALL |



Co-funded by the Horizon 2020 Framework Programme of the European Union

| | |
|---|---|
| Justification | Section 6.4.1 cites many sources and reasons why multidisciplinary collaboration is desirable, but the main reason is that the Internet, whilst being a technological communication channel, has far-reaching impacts that are in the domains of law, social science, humanities, psychology etc. Therefore, in order to promote a human-centric Internet, multidisciplinary collaboration is seen as critically important.<br><br>ICT-28 also contains one Coordination and Support Action aimed at promoting community building between multi-disciplinary researchers, industry and other interested parties to enable cross-disciplinary collaboration in the creation of new patterns for social networks. This clearly is in line with the key observation that multidisciplinary collaboration (Section 6.4.1) is critical for much future NGI development. |

| Title | Help different industries and projects speak to each other |
|---|---|
| Objective | To build an effective community of multiple types of stakeholders and to reap the benefits of such a community. |
| Action | Continue efforts in community building and support. The further step towards a holistic partner ecosystem paradigm is now the creation of connections between different and potentially far domains and industries, fostering knowledge and information sharing, while creating the basis for synergies and complementarities between different sectors. Concrete suggestions include the following.<br>• Continue to support the different cascade funding projects sharing ideas and approaches<br>• Facilitate the interaction between companies targeting different industries and with separate product/service portfolio.<br>• Continue to organise events featuring interesting and diverse Internet-related subject matter so as to attract a wide variety of attendees. Facilitate networking at these events through e.g. interactive games to encourage discussions and contact building.<br>• Utilise tools such as the NGI online map as a one-stop-shop to enable the discovery of new potential partners. |
| Timescale | 2019 and ongoing. This is partially covered by work of NGI Outreach office. |
| Justification | As discussed in Section 6.4.2.2, the importance of a solid partner ecosystem is clear among NGI initiatives. The efforts put in place by the European Commission to foster the creation of new partnerships and networks among technology providers, end-user communities and public institutions in recent years have been massive and their effectiveness is recognized when also speaking with NGI initiatives. A cross-fertilization between industries and technology domains, could enable innovative ideas and unexpected technology applications and use cases, while opening new business opportunities. |

### 3.3.2 Innovation Support

| Title | Foster NGI Initiatives' Go-To-Market Effectiveness |
|---|---|
| Objective | To help bridge the so-called “innovation gap” between research results and innovative products and services that are commercially marketed. |



Co-funded by the Horizon 2020 Framework Programme of the European Union

| | |
|---|---|
| Action | Support NGI initiatives to translate research results into products and services for sale in the market. Suggested actions are as follows.<br>• Organisation of technology, industry-specific and end-user-oriented events that could facilitate an interaction with targeted industries<br>• Marketing support both in terms of market visibility enablement activities and customer needs understanding<br>• Support in cross-countries activities, opening initiatives' addressable market to broader scenarios. |
| Timescale | 2019 and beyond. |
| Justification | As discussed in Section 6.4.2.2, one of the key needs for NGI initiatives, especially for those technology and solution providers at their early business stage, is a further support in go-to-market activities and sales effectiveness, helping start-ups and SMEs move from a fully-funded projects status to solid commercial entities. Facilitating access to funding programs and participation from start-ups is another area where there is space for improvement, according to respondents' feedback. |

| Title | Support Testing and Scalability for Innovation, Research & Development |
|---|---|
| Objective | To help innovators test & evaluate their developments at scale in laboratory and realistic conditions. |
| Action | Continue to provide shared infrastructures, tools and data that can be leveraged by innovative companies, especially SMEs, in order to validate their technologies and turn their proofs of concept into market ready products. Sharing infrastructures and tools can help these companies to cut down their fixed costs and develop their innovations rapidly. |
| Timescale | Ongoing |
| Justification | As discussed in Section 6.4.2.2, fostering scalability, reliability and interoperability is the following step for ensuring technology development and this is another aspect where EC can reinforce its actions. Promoting a trustworthy environment where technology standards and open source models help build on each other progresses in a cumulative way is a win-win approach that the EC should encourage more in the future. |

| Title | Fast-Turnaround SME-Specific Open Calls |
|---|---|
| Objective | To enable SMEs to benefit from cascade funding open calls. |
| Action | Flexible operation of open calls with short turnaround times for funding decisions are needed to enable SMEs to fully benefit. |
| Timescale | ASAP. This is already being investigated and evaluated in H2020 Fed4FIRE+, based on recommendations from HUB4NGI. Results of this investigation are forthcoming, so when they are ready they should be examined for lessons learned. |
| Justification | As discussed in Section 6.4.3, SMEs need to operate in a highly agile way, so three-month cycles for funding decisions are likely to be too long-term for them – they need a decision within a much shorter time period. The traditional Open Call time frames are much too long, with a typical time of three months between the application and the decision, so a different type of Open Call is needed, specifically targeting SMEs and with a fast decision turnaround time. |



Co-funded by the Horizon 2020
Framework Programme of the European Union

| Title | Open-Access Experimentation with Funded Support |
|---|---|
| Objective | To incentivise experimentation facilities to run more experiments and provide more useful services to users. |
| Action | Enhance open access to experimentation facilities, where the experimentation facilities who serve experimenters best are funded, but the experimenters need to fund their own time. This means that the most-used facilities are rewarded financially, so are encouraged to provide useful services that experimenters want to use even without their time being funded, and there is no cost of supporting the experimenters. |
| Timescale | It is recommended that this pattern be evaluated within the H2020 Fed4FIRE+ project. |
| Justification | The current situation is that there are open calls, where often experimenters and the facilities they use are funded for an experiment, and open access, where neither are funded but the facilities are expected to cover the costs of supporting experimenters. This situation is not attractive to experimentation facilities, as it means the more experimenters they are expected to serve, the more stretched they will be. It is recommended therefore to enhance the concept of "open access" to enable the facilities' costs to be covered for each experiment they support, so that all facilities are given the incentive to be successful (i.e. to support more experiments), and the more successful facilities are rewarded financially, promoting a "survival of the fittest" culture. |

| Title | Explore Other Types of Cascade Funding |
|---|---|
| Objective | To increase the impact of the cascade funding mechanism by investigating different ways it can be beneficial. |
| Action | Cascade funding is a useful way of quickly funding small projects, with lightweight administration. Currently this is mainly Open Calls for e.g. close to market projects in ICT-24 and experiments in projects such as Fed4FIRE+. It is recommended that explorations into other types of work that can be commissioned and funded using the cascade funding mechanism be conducted, to fully exploit the power of the mechanism. Suggestions for possible types of work that could be funded using cascade funding include:<br>• Case Studies<br>• Creation of reference data sets<br>• Specific surveys and questionnaires<br>• Experiments beyond those supported in FIRE |
| Timescale | Ongoing |
| Justification | The current focus of the cascade funding ICT24 topic is close to market innovation, but there are other opportunities for flexibly funding short-term smaller-sized pieces of work such as experiments testing specific hypotheses, surveys or interviews gathering opinions or case studies describing a particular situation. The funding can be administered by a parent project, which has a specific theme as is currently in the ICT24 pattern, and the parent project can run open calls for short-term experiments, surveys or case studies and collate, analyse and synthesise the results of the case studies and experiments. It should be a condition of funding these |



Co-funded by the Horizon 2020 Framework Programme of the European Union

| | |
|---|---|
| | experiments, surveys etc, that any data resulting from them must be published as Open Research Data. |

### 3.3.3 Technology Support

| Title | Support Research and Innovation in Key Identified Technology Areas |
|---|---|
| Objective | To continue to support research and innovation in key technology areas identified by the community. |
| Action | Continue to support research and innovation in IoT, AI, Cyber Security, Privacy and Open Data. |
| Timescale | Ongoing |
| Justification | As discussed in Section 6.4.2.2, technologies such as IoT, Artificial Intelligence, 5G, Cybersecurity/Privacy and Open Data were highly recommended by the surveyed NGI initiatives as those areas where EC activities should focus more in the future. This highlights how these technologies, already in the NGI scope, are extremely valuable for EU organisations. |

| Title | Continue to Support Useful Established Technologies |
|---|---|
| Objective | To continue to support technologies that are clearly useful, but not prominent in the hype. |
| Action | Continue to support technologies that have demonstrated usefulness but are not currently trending, such as big data, visualization tools, cloud, intellectual property and digital copyright and e-learning. |
| Timescale | Ongoing |
| Justification | As discussed in Section 6.4.2.2, medium relevance resulted for more established technologies such as big data, visualization tools, cloud, intellectual property and digital copyright and e-learning. Most of these technologies represent key enablers for emerging technologies development. This suggests to EC that keeping an eye on the enabling infrastructure and tools is important. |

| Title | Keep Scanning the Horizon |
|---|---|
| Objective | To keep well informed of emerging technologies and application cases. |
| Action | Continue to fund forward-looking initiatives such as CSAs that investigate emerging technologies, threats, challenges and new opportunities for the NGI. Fund multiple instances of these initiatives, who have different perspectives and utilise different techniques, so as to provide a spectrum of viewpoints. |
| Timescale | Ongoing |
| Justification | As discussed in Section 6.4.2.2, other emerging topics and technologies were mentioned by NGI initiatives as possible areas that EC should take care of in the future. Some of these emerging trends are edge computing, digital fight to fake news, personal data digital twins, neuromorphic computing, quantum computing, and bio-engineering. Furthermore, what emerged as crucial particularly for these emerging topics is keeping focusing on large |



Co-funded by the Horizon 2020 Framework Programme of the European Union

| | |
|---|---|
| | experimentation and testing in a semi-real environment to ensure commercial success of new products and bridge the gap between market and research. |

### 3.3.4 Sustainable Development

| Title | Keep Pushing Sustainable Development |
|---|---|
| Objective | To support the ideals of sustainable development. |
| Action | Continue to incentivize sustainable innovation through dedicated actions, policies and innovation programmes. Active monitoring of progresses towards specific targets is recommended. |
| Timescale | Ongoing |
| Justification | There is considerable evidence that governments are under significant pressure from multiple factors, including increasing urbanization, an ageing population, waste of finite resources, growing inequalities etc. New technologies are increasingly playing an important role in addressing several of these societal challenges. The European Commission has already fully embraced and actively committed to the 2030 Agenda and the 17 sustainable development goals launched by the UN. However, the journey towards a sustainable Europe is only at the beginning, continuing supporting this vision is essential to progress along this way. |

## 3.4 ROADMAP SUMMARY

This section wraps up the roadmap with two diagrams showing the recommended actions in context with each other, time and the NGI Values.

Figure 4 shows the roadmap of recommendations for research and innovation in the NGI that have been described in Section 3.2. The key values (from Section 3.1) are shown at the left and the recommendations in the roadmap are colour-coded to indicate the values they contribute to. Many recommendations contribute to more than one value, and this is indicated by their multi-colour shading. The Roadmap is divided into thematic areas (horizontal groups). Chronologically, the roadmap is divided into two main phases – 2019-2020 (H2020) and 2021 onwards (Horizon Europe). Recommendations for long term or large-scale themes and work programme items are mostly reserved for Horizon Europe, sometimes led by smaller studies in the remaining two years of H2020.

Figure 5 shows the key policy recommendations for implementation of the NGI programme and support of the NGI community that have been described in Section 3.3. These recommendations are not time-dependent, rather they are ongoing, and ideally should start as soon as possible, so they are shown as across the remainder of H2020 and into Horizon Europe. The recommendations are grouped into the thematic groups as described in Section 3.3.



Co-funded by the Horizon 2020 Framework Programme of the European Union

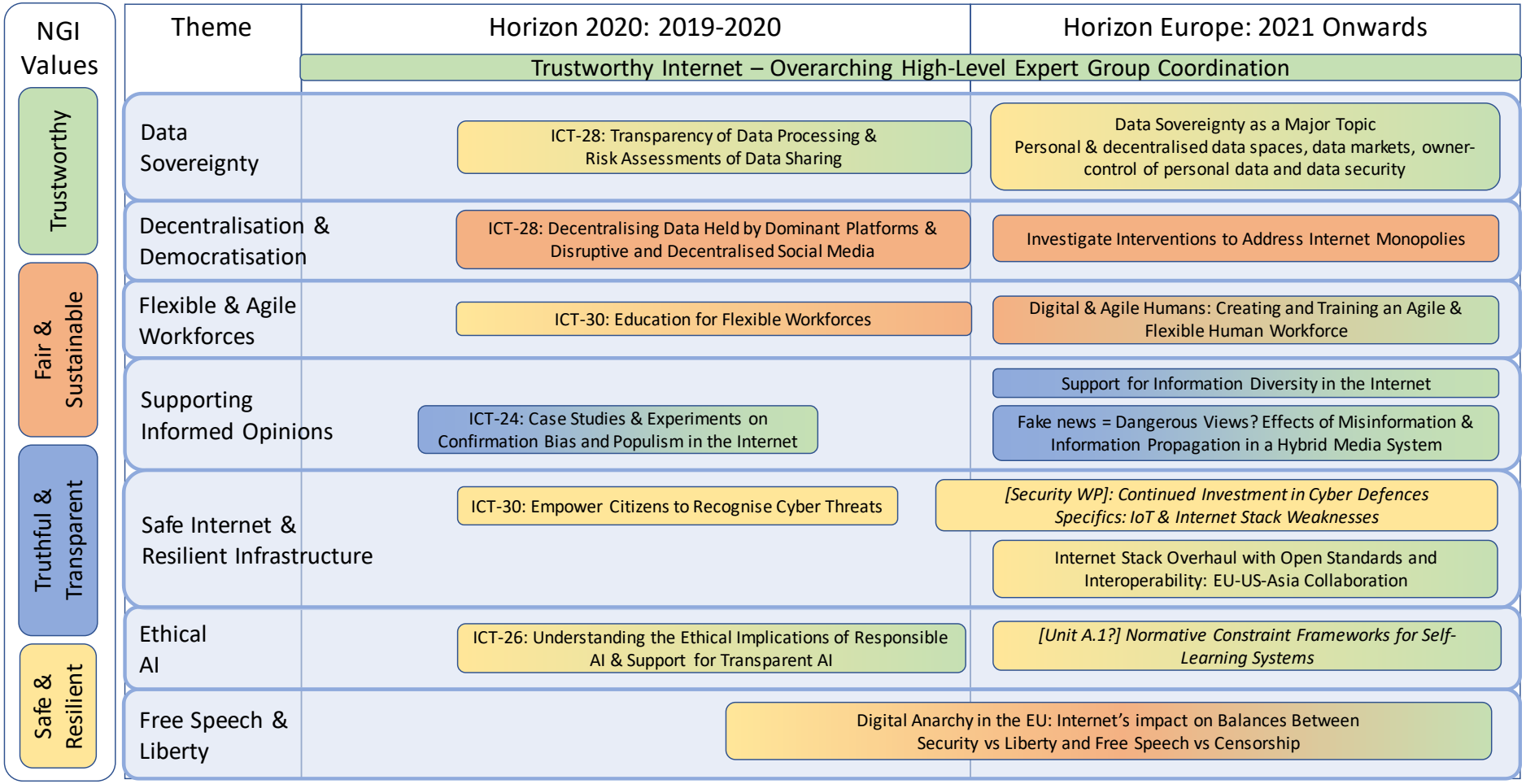


FIGURE 4: ROADMAP FOR RESEARCH AND INNOVATION IN THE NGI





Co-funded by the Horizon 2020 Framework Programme of the European Union

| Theme | Horizon 2020: 2019-2020 | Horizon Europe: 2021 Onwards |
|---|---|---|
| Multidisciplinary Collaboration & Community Support | Support Multidisciplinary Collaboration: Networking Events, Participation Portals, Innovation Hubs, Funding Conditions | |
| | Continue Supporting the NGI Community Cascade Funding Projects Building Communities, Events, Online Directories | |
| Innovation Support | Support NGI initiatives to translate research results into commercial products and services: Collaboration Events, Marketing Support, Cross-National Support | |
| | Provide shared infrastructures, tools and data to support innovation: Validation of ideas, Scalability Testing, Help innovators their turn their proofs of concept into market ready products | |
| | Open Call & Open Access Enhancements Fast-Turnaround SME Calls, Open Access with Funded Support | |
| | Explore Other Types of Cascade Funding e.g. Case Studies, Reference Data Sets, Specific Surveys & Questionnaires, All Kinds of Experiments | |
| Technology Support | Support research and innovation in key technology areas identified by the community | |
| | Continue to support innovation using established technologies | |
| | Keep funding horizon scanning projects | |
| Sustainable Development | Continue to incentivise sustainable innovation through dedicated actions, policies and innovation programmes | |

FIGURE 5: KEY NGI POLICY, IMPLEMENTATION & SUPPORT RECOMMENDATIONS





Co-funded by the Horizon 2020 Framework Programme of the European Union

# 4 NGI FUTURE - DESTINATION HORIZON EUROPE

To specify in more details the longer-term research agenda beyond Horizon 2020, one must take account the fact NGI will become a much larger initiative extending the scope of the current NGI Unit. The “Next Generation Internet” is indeed an Area of Intervention in the Cluster “Digital and Industry” of the proposed Specific Program of Horizon Europe [22]. While details of the Specific Program are still under discussion between the EU Commission, the EU Parliament and EU Member States, a first high-level perspective has been presented by the EC in the last months of 2018 - see Figure 6.

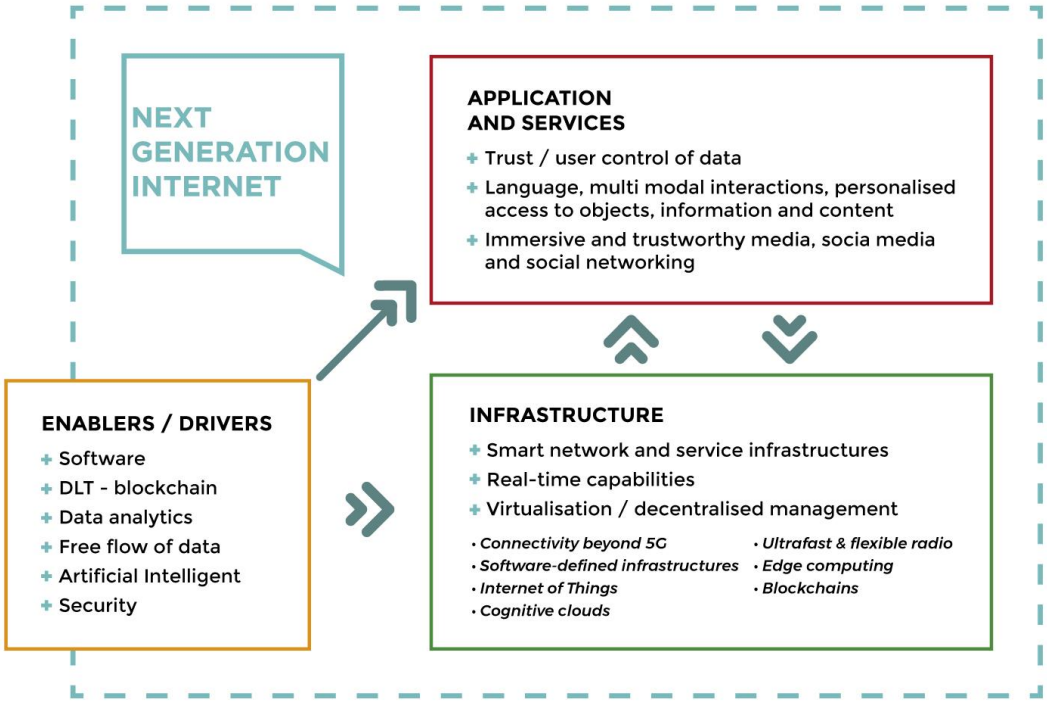


FIGURE 6: NGI PROPOSED STRUCTURE IN HORIZON EUROPE

Europe aims to take the lead in driving efforts that boost EU industrial competitiveness in the global economy. As depicted in Figure 6, the NGI Horizon Europe vision relies on:

- **Smart connectivity/infrastructures**. Concepts, technologies and solutions for trusted and energy-efficient smart network and service infrastructures (connectivity beyond 5G, software defined infrastructures, cognitive clouds), enabling real-time capabilities, virtualisation and decentralised resource management (ultrafast and flexible radio, edge computing, etc.).
- **Smart applications and services** building on trust, interoperability, user control of data, transparent language access, new multi-modal interaction concepts, inclusive and highly personalised access to information, content and objects, including immersive and trustworthy media, social media and networks.
- **Smart enablers,** including software-based middleware, including distributed ledger technologies, working in highly distributed environments, facilitating data mapping and data transfer across hybrid infrastructures with inherent data protection, embedding AI, predictive analytics, security and control which are crucial for free flow of data and knowledge.

In line with this vision, NGI future research and innovation directions will have to embrace a broader set of challenges. While an exhaustive and more detailed analysis of the envisioned



Co-funded by the Horizon 2020 Framework Programme of the European Union

structure for Horizon Europe goes beyond the HUB4NGI project scope, a few core aspects, based on recent reports [23][24][25][26] combined with the work and learnings of the last two years, are summarised hereby.

- **End-to-end systems design** (with few larger infrastructures including international dimension) based on open global standards and standardised interfaces/APIs, where 5G, IoT, edge computing and even autonomous connection mechanisms between edges w/o connection to core network enables for high performing and pervasive networks.
- **New protocols need to be developed to go beyond current TCP/IP limitations**: an end-to-end architecture, including optical networks, needs to support IoT, media and new innovative services over fixed and mobile networks.
- **End-to-end network and protocol validation and interoperability tests** should include real life experimental environments in an early phase of development and include activities to provide fast feedback and to improve the quality of models and simulations.
- **Evolution of experimentation-driven efforts,** through small to large scale testbeds integrating IoT, 5G, Big Data, Edge Computing, etc. for the development of a variety of applications and services across several vertical segments (e.g., media, health, transport, automotive, etc.), requiring by design multidisciplinary approaches.
- **Efforts like Fed4FIRE+, Large Scale IoT Pilots and 5G Testing Pilots** recently started are key to ensure new concepts, technologies, protocols, etc., can be tested. Such pilots enable prototyping for rapid innovations but are also acting as catalyst for the creation of ecosystems embracing different communities.
- **Cascade funding** should continue to create interest for innovative SMEs, Start-ups and business verticals (e.g. Health, Automotive, Media, etc.) to join these pilots and inject into the development and deployment of new concepts, mechanisms and technologies.
- **Multi-actor governance protocols/system design principles and methodologies** for cooperating robots, sensors, devices and people should be investigated as key to understand the challenges and implications related to Collective Human Experience (ethics, security, privacy concerns) in highly immersive scenarios.
- **Collective intelligence/behaviour**: While psychological, societal and cultural structures and processes, including changes in identity and in cognition/rationality, are important factors for collective intelligence and networked personalities, deep attention should be paid to user group perspectives with recognition of distinctions within them and questions around inclusion and risks of exclusion.
- **Self-governing infrastructures.** The Internet backbone is more and more fragmented and may increasingly manifest itself into multiple autonomous “internets”, in which different service providers are creating private islands that goes from cloud to satellite. The way in which this integration will work still need lots of research, as well as how the movement from one “island” to another will work. Increasingly, autonomous and goal-driven AI mechanisms are expected to enforce different degrees of self-governance mechanisms.
- **Big Data Analytics**. While the global amount of data generated worldwide is rising exponentially, especially thanks to the increasing IoT deployments across many sectors, currently only a small amount of this data is analysed for service/value creation [27][28][29]. This is predicted to change thanks to several converging factors: high performance computing capabilities (data processing), better performant communication networks (data transport) and increasing adoption of cognitive/AI capabilities (intelligent/predictive data analytics). In this area, further research is required to understand the challenges and opportunities related to data capture, storage, manipulation, management, analysis, knowledge extraction, security, privacy and visualisation [30].



Co-funded by the Horizon 2020
Framework Programme of the European Union

# 5 CONCLUSIONS

This deliverable has analysed critical aspects that need to be addressed in order to shape the Internet of the future in a more open, inclusive, secure, trusted and decentralised way. It provides a summary of recommendations from the perspective of the HUB4NGI CSA, cast into the form of a roadmap of recommendations that is intended as input to the processes that determine the upcoming work programme for the Next Generation Internet.

The key guiding principle underpinning the roadmap is that the Next Generation Internet is human-centric. The methodology adopted in this deliverable has taken this principle to heart, and as a result this deliverable has expanded on the NGI Vision and determined human-centric values for the NGI that protect human rights and freedoms, which are presented in the roadmap as aspirational goals for the NGI. These NGI Values are: *Trustworthiness*, *Safety & Resilience*, *Truthfulness & Transparency* and *Fairness & Sustainability*.

Even though the Internet benefits many people, it hosts many threats and challenges that can violate, inhibit or impede human rights and freedoms represented by the NGI Values, and addressing these challenges forms the basis for the recommendations. The recommendations are presented in two key areas: firstly, recommendations for research and innovation and secondly policy recommendations for implementation & management of the NGI Programme. These have been described in the detailed roadmap section and summarised at the beginning of this document along with a roadmap diagram showing how they are integrated.



Co-funded by the Horizon 2020
Framework Programme of the European Union

# 6 APPENDICES – DETAILS OF ANALYSES SUPPORTING ROADMAP

These appendices contain detailed analysis that support the roadmap described in the main body of the deliverable. They are arranged in the same order as the methodology, beginning with the values underpinning a human-centric Internet, then threats and impediments are identified from HUB4NGI and external work that represent challenges to these values. Next, a gap analysis of the current work programme is presented to determine the recommendations for research and innovation (which have already been presented in Section 3.2 in the main body of the document). Finally, experiences from HUB4NGI (and reported in other deliverables) have been summarised to determine recommendations for support of the NGI community and for improvements to the implementation of the programme (also presented in Section 3.3).

In addition to the work from HUB4NGI, these appendices have drawn from several external sources. HUB4NGI D2.1 provided an examination of recent sources at the time of its writing with a view to understanding the key themes concerning the Internet's impact on society, as well as providing recommendations for research to address issues. These appendices provide an update of D2.1 by analysing key high-level additional sources to provide a comparison point to the recommendations from HUB4NGI work that are described in later sections. The sources are briefly discussed below and were chosen as they are comprehensive and wide-ranging in their scope. They are complementary in that they provide an analysis of the impact of the Internet on human rights, a high-level socio-economic perspective, a high-level technical perspective, together with a specific focus on media.

- The United Nations **Universal Declaration of Human Rights** (UDHR) [6] is the world-famous statement of human rights as an aspiration for all nations. Given that the NGI aims to be a human-centric Internet, the UDHR provides the basis for the rights and freedoms that the NGI should uphold.
- **The 2017 Internet Society (ISOC) Global Internet Report: Paths to Our Digital Future** [1] is the fourth annual Global Internet Report and examines the future of the Internet from a predominantly socio-economic perspective[3].
- **The Next Generation Internet 2025: A study prepared for the European Commission DG Communications Networks, Content & Technology** [2] is a commissioned report authored by Gartner and the NLnet Foundation. It is predominantly an examination of the technical developments and needs of the Internet infrastructure. This provides a technical counterpart to the socio-economic viewpoint of the ISOC Global Internet Report.
- **The Future of Media Innovation, European Research Beyond 2020** [7] is a vision paper from the Mediaroad EU project. Its contribution to this study is its focus on the media in the Internet and how it is evolving.

This section contains three main subsections: trends & threats with analysis on the needed work to address the threats, principles guiding the implementation of the NGI, and human-centric values for the NGI.

[3] The 2017 report is the latest at the time of writing. A 2018 Internet Society Global Internet Report is expected, but as of Dec 2018, is not published.



Co-funded by the Horizon 2020 Framework Programme of the European Union

## 6.1 APPENDIX 1: A HUMAN-CENTRIC INTERNET: THE INTERNET & THE UNIVERSAL DECLARATION OF HUMAN RIGHTS

Given the prominence of threats to personal freedoms and rights and the guiding principle that the NGI is a human-centric Internet, stakeholders using the NGI must understand and be incentivised to respect human freedoms and rights. The *de facto* starting point for discussions regarding human rights is the United Nations Declaration of Human Rights (UDHR) [6], and therefore the relevant articles from the UDHR that concern the NGI are presented here with discussion regarding the issues surrounding them. This discussion will feed into human-centric values that will be presented in the Roadmap section, and these serve as more detailed guiding principles beneath the overarching human-centric Internet, and can serve as objectives guiding the direction of the NGI

### 6.1.1 Article 12: The Right to Privacy & Reputation

> *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks. [6]*

Violations of privacy over the Internet are clearly a major threat, and this has been identified in the work programme as well as in the sources. Personal data clearly needs protecting, and its owners need to know and be able to control what is happening to it when it is accessible by third parties. There are clear threats towards privacy if norms, regulations, practices and security controls do not limit the gold rush towards exploitation of data.

### 6.1.2 Article 17: The Right to Property & Protection from Theft

> *(1) Everyone has the right to own property alone as well as in association with others.*
>
> *(2) No one shall be arbitrarily deprived of his property. [6]*

Personal and other data should be regarded as property, but clearly data is different to physical property in that data can be taken without the owner losing it (e.g. leaked or copied). The current thinking that "data is the new oil" only holds true considering the attitude towards the commoditisation of data (because unlike oil, data is *ad infinitum* reproducible), but the owner of data can be damaged via leaks of the information contained within that data (e.g. as a violation of privacy), and they also can be deprived of data if it is compromised or lost when stored by a third party.

### 6.1.3 Article 19: The Right to Freedom of Expression

> *Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers. [6]*

This right represents a critical conflict in the debates around the perversion of opinion through e.g. populist leaders spreading fake news. One the one hand, everyone has the right to *"impart information and ideas"*, but on the other hand information manipulators can claim this right to be a justification for the spreading of misinformation – they can claim that they are simply disseminating ideas. Censorship and control of information are mechanisms to combat misinformation, but clearly these mechanisms can inhibit the right to freedom of expression.



Co-funded by the Horizon 2020 Framework Programme of the European Union

### 6.1.4 Article 21: The Right to Democratic Government

> *(1) Everyone has the right to take part in the government of his country, directly or through freely chosen representatives.*
>
> *(2) Everyone has the right of equal access to public service in his country.*
>
> *(3) The will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret vote or by equivalent free voting procedures. [6]*

The main point of concern to the NGI is 21.3, which mandates the free and fair election of governments based on the will of the people. Given recent events where elections have been tainted with suspicions of manipulation, there is a hypothesis that there is a causal link between misinformation and its effects on the will of the people as expressed in their voting. This hypothesis needs testing as part of a more general study of the Internet's contribution to opinion perversion and what tangible effects it can cause.

### 6.1.5 Article 23: The Right to Employment

> *(1) Everyone has the right to work, to free choice of employment, to just and favourable conditions of work and to protection against unemployment.*
>
> *(2) Everyone, without any discrimination, has the right to equal pay for equal work.*
>
> *(3) Everyone who works has the right to just and favourable remuneration ensuring for himself and his family an existence worthy of human dignity, and supplemented, if necessary, by other means of social protection.*
>
> *(4) Everyone has the right to form and to join trade unions for the protection of his interests. [6]*

Given that there are threats to employment from the automation brought about by technologies in the NGI and AI, the major relevant points here are 23.1, concerning the right to work for all people and 23.3, the right for fair pay and supplementary social protection.

The question of the division of labour between human and machine has been faced throughout history whenever disruptive technical innovations have occurred[4], and society has adapted to accommodate the new technological step change, but the current situation is complicated by the speed of change, a case in point being in AI. We are not currently anywhere near the level of superintelligence (i.e. intelligence greater than that of a human), but if AI machines can adapt, learn from their environments and spawn more intelligent versions of themselves, the pace of change can accelerate. If the machines become ever more capable and replace workers at a rate faster than roles can be found that human workers can be retrained to fill, mass unemployment will result.

The key question is how to create a flexible labour economy, where both humans and automation contribute by utilising their respective strengths. It is well understood where humans' machines' respective strengths lie at the current time, but society needs to track technological development (in particular AI) to make sure these principles still hold true. All the while, we need

[4] Examples are the communication revolution brought about by the invention of the Gutenberg press, or the agricultural revolution started by the invention of the threshing machine. In both cases, there was temporary upheaval – in the first case, mass communication was suddenly possible where previously it was the privilege of the extremely wealthy who could afford literature created by hand; and in the second case, a human task was automated with threats to farm workers livelihoods, and there were riots where farm workers destroyed threshing machines.



Co-funded by the Horizon 2020
Framework Programme of the European Union

to understand which combinations of human skill and machine ability will provide a sustainable future, where both labour forces are accommodated and valued.

### 6.1.6 Article 26: The Right to Education

> *(1) Everyone has the right to education. Education shall be free, at least in the elementary and fundamental stages. Elementary education shall be compulsory. Technical and professional education shall be made generally available and higher education shall be equally accessible to all on the basis of merit.*
>
> *(2) Education shall be directed to the full development of the human personality and to the strengthening of respect for human rights and fundamental freedoms. It shall promote understanding, tolerance and friendship among all nations, racial or religious groups, and shall further the activities of the United Nations for the maintenance of peace.*
>
> *(3) Parents have a prior right to choose the kind of education that shall be given to their children. [6]*

Here, the main point of relevance to the NGI is 26.2, which describes the direction that education must follow: to promote the *"strengthening of respect for human rights and fundamental freedoms"* and *"understanding, tolerance and friendship"*. There is clearly a threat to these principles, in that the Internet is a highly efficient communication channel that can carry targeted misinformation; and can provide fora and mechanisms exacerbating confirmation bias (the so-called "echo chambers"), which can lead directly to polarisation, intolerance and extremism. These phenomena also undermine human enlightenment and curiosity by the reduction of open-mindedness and the promotion of simplistic messages. It is an obvious priority that the NGI should direct effort at addressing the forms of misinformation, opinion perversion and confirmation bias that contradict the principles of curiosity, open-mindedness, understanding, tolerance and friendship.

### 6.1.7 Article 29: Responsibility to the Community & Legitimate Limitations of Rights and Freedoms

> *(1) Everyone has duties to the community in which alone the free and full development of his personality is possible.*
>
> *(2) In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society.*
>
> *(3) These rights and freedoms may in no case be exercised contrary to the purposes and principles of the United Nations. [6]*

The main concern to the NGI here is 29.2, which discusses the acceptable cases for limitations of rights and freedoms. Here, the limitations serve to preserve the rights and freedoms of others and to uphold the morality, public order and general welfare of a democratic society. Even though the article specifically refers to a democratic society, this point can be used as justification for limitations on the rights and freedoms of citizens by e.g. authoritarian governments in the name of public order, national security or the "greater good". Manifestations of these limitations can include surveillance (itself an invasion of the right of privacy) or profiling, which can lead to active limitations of freedoms such as arrest or imprisonment.



Co-funded by the Horizon 2020 Framework Programme of the European Union

This is very obviously the perennial “national security vs liberty” debate, and clearly the Internet provides opportunities, mechanisms and channels for infringements of personal freedoms and rights under the pretext of protecting a nation or its population. Studies of “security vs liberty” cases with a special focus on the contribution of the Internet’s channels and stakeholders need to be undertaken from a multidisciplinary legal, ethical and socio-economic (ELSE) perspective.

## 6.2 APPENDIX 2: THREATS & IMPEDIMENTS TO A HUMAN-CENTRIC INTERNET

It is clear that while the Internet has many benefits, threats are many and varied, and need to be addressed in order that people and society are not damaged as a result of their using the Internet, and to achieve the promised benefits. Threats are to different entities, e.g. people or nations, but for the vast majority, a threat will have either a direct or indirect impact on the rights of people, inhibiting or violating their rights. In some cases, threats are in conflict – i.e. the mitigation of a threat by one party threatens another.

Several strong trends and threats have emerged from analysis of D2.1 results and the additional sources, and this section discusses the major themes. For each trend & threat, a summary is presented, supported by quotations from the sources, and followed by an analysis of the needed research and innovation to address the issues presented. These needs will be developed in the roadmap section in terms of recommendations.

### 6.2.1 Decline of Public Trust in the Internet

Public trust is declining in the Internet, due to varied threats to citizens’ liberty, privacy and equality. Widely publicised stories of data breaches, large platforms operating profiling and governments using the Internet for surveillance on citizens, coupled with perceived abuses of personal data, are having the consequence that the public are becoming more conscious that their privacy is at risk and their activities are being monitored through their use of the Internet.

> *[…] an ever-growing trend that citizens are becoming less trustful and more aware of the dangers in the Internet. [3]*
>
> *As the scope and severity of cyber threats intensifies, and as global Internet platforms are used to deliberately spread disinformation, users will lose trust in the Internet. […] With greater amounts of data being collected about many more aspects of our lives, we will have even more to lose in future data breaches. If the burden of risk is not more widely shared — through clearer legal accountability and greater investments in security — the decline in overall trust will accelerate. [1]*

***Needs***

Trustworthiness in the Internet clearly needs addressing and is multifaceted – i.e. there are many aspects that can reduce the level of trust in the Internet. Overall, there is a need for a coordinated programme of multidisciplinary work, aiming to address multiple aspects of trust in the Internet.

A major focus of mistrust is not on the Internet infrastructure itself here but on individuals, companies, governments or other organisations who use the Internet in ways that citizens find concerning – for example, major Internet companies are facing public scrutiny and a backlash of public opinion regarding their actions, and this has clearly impacted their trustworthiness. This reflects onto the Internet itself – it is in danger of getting a reputation as a “wild west” where users need to tread carefully, and their actions may have consequences that may not be immediately apparent but can be highly damaging.



Co-funded by the Horizon 2020 Framework Programme of the European Union

Users who are uneducated as to the dangers and pitfalls of their use of the Internet are particularly vulnerable, and newspaper stories of "cyber victims" further undermine public trust. There is clearly a need to address the challenge of uneven education regarding the risks of using the Internet for all citizens.

### 6.2.2 Accelerating Proliferation of Cyber Threats

The acceleration of cyber threats is clearly a major concern to the wellbeing of Internet users, and violates their right to privacy or the ownership of data. It is therefore an obvious priority to monitor the development and propagation of cyber threats and create planned countermeasures and defences.

> *Perhaps the most pressing danger to the future of the Internet is the rising scope and breadth of Cyber Threats. […] Insufficient attention to security will undermine trust in the Internet. Indeed, human safety is at stake […] The scale of cyberattacks is steadily growing, and many anticipate the likelihood of catastrophic cyberattacks in the future. We already see attacks on a national scale, so it is not farfetched to imagine a digital pandemic with attacks crippling entire economies. As one North American industry analyst put it, a "digital Pearl Harbor is coming …" [1]*

The Internet is now a sufficiently valuable and critical to society that it can be classed as a domain of warfare, and an "arms race" is predicted between the attackers and the cyber security specialists who are creating technology and operational methods to combat the cyber-attacks.

> *As the Internet becomes intertwined with national security, cyber offense and defense strategies will shape the future Internet for industry and individual users alike. Cyberspace is now considered the fifth domain of warfare, but there are few agreed rules of engagement. […] Cybersecurity will be the most pressing challenge of the next decade; responses to date have been thoroughly insufficient and the costs are escalating. […] All our survey respondents, across stakeholder groups and regions, expect to see high investment and innovation in Internet security in the future. [1]*

Recent targets of cyber-attacks have been aimed at undermining governance structures and public services (for example the 2017 "WannaCry" attack on the UK National Health Service[5]), which reinforces the message that society is critically dependent on computer systems and the Internet, and that the Internet is also a channel for attack. Further, weaknesses in the lower layers of the Internet are well known and are a significant target for exploitation.

> *Recent cyberattacks that appear to be designed to destabilise political systems are especially alarming and point to a future in which undermining governance structures, and therefore the values that they stand, for will become more commonplace. [1]*
>
> *[…] fragility, lack of trust and confidentiality, and generally weak defence characteristics of the first generation internet. [2]*

The Internet of Things has had strong growth in recent years, with many types of devices connected.

> *We can expect the world to change fundamentally over the next five to seven years with the convergence of the Internet and Physical Worlds and the deployment of the Internet of Things (IoT). When everything that can be connected is connected, whole economies and societies will be transformed.*

[5] https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/



Co-funded by the Horizon 2020 Framework Programme of the European Union

> *Services will become more efficient and data driven, providing new ways for us to interact with the world around us. However, increased security threats and device vulnerabilities, as well as incompatible standards and a lack of interoperable systems, could well undermine the technology's promise. Without appropriate safeguards and deliberate efforts to ensure transparency and user control, IoT could drive data collection and use in ways that further undermine privacy. [1]*

Many IoT devices are single-purpose, created for one application only and with little thought for security. Some of these devices are in the home, within private networks and inside firewalls, leading to fears of surveillance or attacks from within if these devices are compromised.

> *A major security concern is the Internet of Things. This encompasses a proliferation of devices, whose security provenance and resilience may not be verified. Many IoT devices are created by manufacturers whose expertise lies in areas other than Internet security, and devices may be infrequently or never patched to address security concerns. [3]*

The defences put in place need to be balanced with the liberties of citizens using the Internet.

> *[…] we cannot afford to let the 'securitisation' of the Internet, and our digital lives, run rampant: there is a very real threat that online freedoms and global connectivity will take a back seat to national security. Given the growing pressure from cyber threats and security challenges such as terrorism, the ease with which our open societies and our freedoms and rights could become subordinate to pervasive surveillance regimes facilitated by AI and IoT should not to be underestimated. […] The future of Internet openness will depend on how governments deal with the growing pressure to respond to security challenges. [1]*

The Internet's infrastructure is at risk, because it relies on decades-old protocols. As attacks have become more sophisticated, they have revealed numerous weaknesses in the Internet stack, each of which is vulnerable.

> *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. […] 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 an adequate deployment strategy at the other end is recommended. [2]*

A further threat trend is cyber-attacks aimed at destabilising governance and political systems.

> *Recent cyberattacks that appear to be designed to destabilise political systems are especially alarming and point to a future in which undermining governance structures, and therefore the values that they stand, for will become more commonplace. [1]*

***Needs***



Co-funded by the Horizon 2020 Framework Programme of the European Union

There is a clear need to continue with the investment in research addressing cyber threats, as part of an ongoing battle against the attackers. The current foci are defence against attacks on critical infrastructures, destabilisation of governance and political systems, investigating the threats and weaknesses of IoT devices and addressing weaknesses in lower layers of the Internet, but new threats will continually emerge, and constant vigilance to identify new threats is required.

### 6.2.3 New Digital Divides

The traditionally-defined digital divide, between those that have access to the Internet and those that do not is reducing, presumably through widespread broadband access, but new divides are emerging that inhibit fairness and equality. The divides currently identified include differentiated opportunity potential between those that can adapt to the pace of change in the Internet and those that cannot and divide between those that can protect against cyber-attacks and those that cannot.

> *Data shows that, while we still have a long way to go, the Digital Divides as we have historically defined it — those who have access to the Internet versus those who do not — is closing. […] Divides across society between those who are able to adapt to an ever-changing world and those who are not. […] As society struggles to absorb and adapt to these changes and their ramifications, new divides will appear between those who are suitably trained for current and future employment and those whose employment is dependent upon sectors that are no longer sustainable. […] As new threat vectors emerge, a security divide will materialise between those with the knowledge and resources to protect themselves from cyber threats and those without. [1]*

With the introduction of new patterns such as IoT, edge computing and AI, the Internet is changing, and evidence points to accelerating change in terms of opportunities and threats.

> *The hyperconnected Internet Economy that results will see traditional industries morphing, emerging economies thriving and new market leaders from around the globe driving innovation and entrepreneurship. […] All parts of society — from local communities to education systems, healthcare and public services — will have to adapt to the pace of change. […] The adoption of Artificial Intelligence and the Internet of Things will transform the global economy offering opportunities for the developing world; however, without adequate infrastructure and broader economic opportunity, many nations may be left behind. [1]*

***Needs***

There is a need to investigate programmes that will enable citizens and workforces to address these ever-evolving challenges. Education and economic patterns are key candidate subject areas for these investigations. The key success criterion in this environment is that ability to change to keep pace with the changing environment: that those that fail to adapt will be left behind and uncompetitive. In addition, whole economies will need to change to keep pace.

### 6.2.4 AI Trustworthiness, Responsibility & Accountability

AI systems are becoming more mainstream but there are fears regarding their controllability, responsibility & accountability.

> *[…] advancements in AI and IoT may threaten human rights and personal freedoms and have huge implications for the transparency of decision making and expectations of privacy. Algorithms use enormous quantities of information, much of it collected in ways that are not transparent to individuals.*



Co-funded by the Horizon 2020 Framework Programme of the European Union

> *How will we ensure accountability when algorithms make decisions that affect people's lives but are difficult to understand or to appeal? [1]*

The HUB4NGI Responsible AI consultation [4] has also highlighted the need for trustworthy AI, as well as discussing the key factors contributing to a trustworthy AI system.

> *Trustworthiness of an AI system is critical for its widespread acceptance. Transparent justification of an AI system's decisions, as well as other factors such as provenance information for its training data, a track record of reliability and comprehensibility of its behaviour, all contribute to trustworthiness. [4]*

The consultation report compared the consultation's results against three other initiatives and reported where there were agreements and differences. These are the EC's "approach on Artificial Intelligence" [14], the European Group on Ethics in Science and New Technologies (EGE)'s [15] Statement on "Artificial Intelligence, Robotics and 'Autonomous' Systems" [16], and the European Economic and Social Committee's opinion statement on the socio-economic consequences of AI [17]. Overall, there is broad agreement between the different studies, and this consultation's themes are shared with the other three studies. Each of the four initiatives covers a different subset of themes and to illustrate the overlaps and gaps, the following table maps the three external sources' areas of concern to this consultation's themes.

TABLE 1: COMPARISON OF KEY AREAS FROM DIFFERENT EUROPEAN AI STUDIES

| *EESC Opinion: Areas "Where AI Poses Societal Challenges"* | *EC Approach* | *EGE Statement* | HUB4NGI Responsible AI Consultation: Themes |
|---|---|---|---|
| Safety | AI Alliance for the future of AI in Europe addresses safety | *… "safety, security, the prevention of harm and the mitigation of risks"* | This is not an explicit theme in the consultation, but safety is a key aspect of the "Regulation & Control" theme. |
| - | Regulation for liability | *… "human moral responsibility"* | Dedicated theme of "Responsibility" |
| Governance and regulation | Investigation into application of existing EU directives and regulations | *… "governance, regulation, design, development, inspection, monitoring, testing and certification"* | Dedicated themes of "Regulation & Control" and "Design" |
| Transparency and accountability | Algorithmic transparency | *… "explainability and transparency of AI and 'autonomous' systems"* | Dedicated theme of "Transparency" |
| Ethics | AI Alliance for the future of AI in Europe addresses ethical issues | The EGE statement is concerned with ethics in AI, Robotics and Autonomous Systems | Dedicated theme of "Ethics" |



Co-funded by the Horizon 2020 Framework Programme of the European Union

| | | | |
|---|---|---|---|
| Education and skills | Support for EU upskilling to use new AI technologies | - | Deskilling and the loss of knowledge are covered in "Socioeconomic Impact" |
| (In)equality and inclusiveness | AI Alliance for the future of AI in Europe addresses inclusiveness | - | Discrimination is covered in "Socioeconomic Impact" |
| Work | - | - | Threats to employment are covered in "Socioeconomic Impact" |
| Privacy | GDPR & AI Alliance for the future of AI in Europe addresses privacy | - | Privacy is covered in "Socioeconomic Impact" |
| Warfare | - | Weapons and the principle of Meaningful Human Control | MHC is advocated in discussion of Responsibility |
| Superintelligence | - | - | Touched on in discussion of Responsibility |
| - | Support for Digital Innovation Hubs (DIH) to foster collaborative AI design | - | "Design" theme – design-time considerations |

***Needs***

In order for AI systems to be trustworthy and accepted into society, the issues regarding responsibility, ethics, accountability, transparency etc will need to be addressed. The key findings of the consultation are listed as follows (reproduced from [4]).

Because of AI's disruptive potential, there are significant, and possibly unknown, ethical implications for AI & autonomous machines, as well as their applications.

- AI research needs to be guided by established ethical norms, and research is needed into new ethical implications of AI, especially considering different application contexts.
- The ethical implications of AI need to be understood and considered by AI researchers and AI application designers.
- The ethical principles that are important may depend strongly on the application context of an AI system, so designers need to understand the expected contexts of use and design with the ethical considerations they give rise to accordingly.



Co-funded by the Horizon 2020 Framework Programme of the European Union

- Ethical principles need not necessarily be explicitly encoded into AI systems, but it is necessary that designers observe ethical norms and consider the ethical impact of an AI system at design time.
- Ethical and practical considerations need to be both considered at an AI system's design time, since they can both affect the design. They may be interdependent, and they may conflict.
- Assessment of the ethical impacts of a machine needs to be undertaken by the moral agent responsible for it. At design time, the responsible moral agent is most likely the designer. At usage time, the responsible moral agent may be the user, and the impacts may depend on the application context.

Considerations regarding transparency, justification and explicability of AI & autonomous machines' decisions and actions are strongly advocated by the panel, in concert with others in the community.

- AI decisions and actions need to be transparent, explained and justified; and the explanation needs to be comprehensible by lay people as AI systems become more exposed to the general public.
- Provenance information regarding both AI decisions and their input data (as well as any training data) needs to be recorded in order to provide an audit trail for an AI decision.
- Trustworthiness of an AI system is critical for its widespread acceptance. Transparent justification of an AI system's decisions, as well as other factors such as provenance information for its training data, a track record of reliability and comprehensibility of its behaviour, all contribute to trustworthiness.

Investigation into regulatory aspects such as law, guidelines and governance is needed – specifically applied to new challenges presented by AI and automated systems. In addition, control aspects need investigation – specifically concerning how AI & automated systems' behaviour may be monitored and if necessary corrected or stopped.

- Certification of "safe AI" and accompanying definitions of safety criteria are recommended. The application context determines the societal impact of an AI system so the safety criteria and resulting certification are likely to depend on the application the AI is put to. New applications of existing AI technology may need new assessment and certification.
- Determination of remedial actions for situations when AI systems malfunction or misbehave is recommended. Failure modes and appropriate remedial actions may already be understood, depending on the application domain where AI is being deployed (e.g. which emergency procedures are needed when a self-driving car crashes may very similar to those needed when a human-driven car crashes), but investigation is needed into what existing remedial actions are appropriate in what situation and whether they need to be augmented.
- An important type of control is human monitoring and constraint of AI systems' behaviour, up to and including kill switches that completely stop the AI system, but these governing mechanisms must fail safe.
- A further choice of control is roll-back of an AI system's decision, so that its direct consequences may be undone. It is recognised that there may also be side or unintended effects of an AI system's decision that may be difficult or impossible to undo, so careful assessment of the full set of implications of an AI system's decisions and actions should be undertaken at design time.
- Understanding of how the law can regulate AI is needed, and as with other fast-developing technology, the law lags technical developments. The application context



Co-funded by the Horizon 2020
Framework Programme of the European Union

may be a major factor in AI regulation, as the application context determines the effects of the AI on society and the environment.

- Even though there has been recent discussion of legal personhood for robots and AI, at the current time and for the foreseeable future, humans need to be ultimately liable for AI systems' actions. The question of which human is liable does need to be investigated however, and each application context may have different factors influencing liability.

AI already has had, and will continue to have, disruptive impact on social and economic factors. The impacts need to be studied, to provide understanding of who will be affected, how they will be affected and how to guard against negative or damaging impacts.

- Understanding of the socioeconomic impacts of AI & autonomous machines on society is needed, especially how AI automation differs from other types of disruptive mechanisation.
- AI's impact on human workers needs to be investigated – how any threats or negative effects such as redundancy or deskilling can be addressed, as well as exploiting any benefits such as working in dangerous environments or performing monotonous tasks and reducing errors.
- Public attitudes towards AI need to be understood, especially concerning the factors that contribute to, and detract from, public trust of AI.
- Public attitudes are also connected with assessment of the threats that AI pose, especially when AI can undermine human values, so investigation is required into how and when AI is either compatible or conflicts with human values, and which specific ones.
- Research is needed into how users of AI can identify and guard against discriminatory effects of AI, for example how users (e.g. citizens) can be educated to recognise discrimination.
- Indirect social effects of AI need to be investigated, as an AI system's decisions may affect not just its users, but others who may not know that they are affected.
- How AI systems integrate with different types of networks (human, machine and human-machine) is an important issue – investigation is needed into an AI system's operational environment to determine the entities it interacts with and affects.
- There is unlikely to be a one-size-fits-all approach to social evaluation of AI and its applications – it is more likely the case that each application context will need to be evaluated individually for social impact, and research is needed on how this evaluation can be performed in each case.

Design-time considerations & patterns for AI & autonomous machines need to be investigated, especially concerning what adaptations to existing design considerations and patterns are needed as a specific result of AI.

- Interdisciplinary teams are necessary for AI and application design to bring together technical developers with experts who can account for the societal, ethical and economic impacts of the AI system under design.
- Ethical principles and socioeconomic impact need to be considered from the outset of AI and application design.
- Whilst the AI design should have benefits for humankind at heart, there will also be cases where non-human entities (e.g. animals or the environment) may also be affected. Ethical principles apply to all kinds of nature, and this is not to be forgotten in the design process.
- Identification and recognition of any bias in training data is important, and any biases made clear to the user population.



Co-funded by the Horizon 2020
Framework Programme of the European Union

Issues and considerations regarding moral and legal responsibility for scenarios involving AI & autonomous machines are regarded as critical, especially when automation is in safety-critical situations or has the potential to cause harm.

- Humans need to be ultimately responsible for the actions of today's AI systems, which are closer to intelligent tools than sentient artificial beings. This is in concert with related work that says, for current AI systems, humans must be in control and be responsible.
- Having established that (in the near term at least) humans are responsible for AI actions, the question of who is responsible for an AI system's actions needs investigation. There are standard mechanisms such as fitness for purpose where the designer is typically responsible, and permissible use where the user is responsible, but each application of an AI system may need a separate assessment because different actors may be responsible in different application context. Indeed, multiple actors can be responsible for different aspects of an application context.
- Should the current predictions of Artificial General Intelligence[6] and Superintelligence[7] become realistic prospects, human responsibility alone may not be adequate and the concept of "AI responsibility" will need research by multidisciplinary teams to understand where responsibility lies when the AI participates in human-machine networks. This will need to include moral responsibility and how this can translate into legal responsibility.

A key overarching theme of this consultation is that it asserts that application contexts are key influencers of many aspects of "Responsible AI", more so than the underlying AI algorithms because the application context determines the societal impact, and whether it is for good or poses risks. Different application contexts may use the same underlying AI algorithms, but the contexts may have totally different risks, stakeholders, ethical considerations and regulation requirements. This correlates with the "AI is a tool" school of thought that says that the use the AI is put to is the subject of ethical concern, regulation and responsibility; rather than the AI algorithm itself. Existing application contexts may have their own regulations and control patterns already, and these can for the basis for AI systems participating in the context. (A key example here is AI-powered self-driving vehicles. There are many regulations and practices for human-driven vehicles, so the question is what need to be changed or added to cater for self-driving vehicles.)

AI has significant potential for disruptive socioeconomic impact. Lessons may be learned from previous examples of disruptive technologies and analogies may be drawn between AI and historical examples of disruptive mechanisation, but an open question remains regarding what sets AI apart from previous examples of technological disruption.

### 6.2.5 Threats of Privacy Violation & Surveillance

Privacy violation and abuse of personal data are major threats, and these can occur in different scenarios and ways, including abuses or theft of personal data, surveillance, profiling of citizens and governments limiting personal freedoms in the name of national security.

> *The future of the Internet is inextricably tied to people's ability to trust it as a means to improve society, empower individuals and enable the enjoyment of Personal Freedoms and Rights. […] the Internet also brings challenges to human rights like privacy and free expression. Technologies like Artificial Intelligence and the Internet of Things will enable the generation and collection of enormous amounts of information about individuals that can be analysed in ways that are deeply personal, raising the potential for a "surveillance society"*

[6] Pennachin, C. ed., 2007. *Artificial general intelligence* (Vol. 2). New York: Springer.
[7] Boström, N., 2014. *Superintelligence: Paths, dangers, strategies*. Oxford University Press.



Co-funded by the Horizon 2020 Framework Programme of the European Union

> *to emerge. […] Without a change of course, personal freedoms and rights online may well be nearing a point of irreversible decline. [1]*

There is now mainstream public acceptance that privacy is becoming a major concern for citizens. In the wake of scandals such as the Cambridge Analytica scandal[8], there has been a backlash against large platforms that collect personal data, which has contributed to a decline in trust of them.

> *The 2017 CIGI/IPSOS study revealed that: "A majority of global citizens are more concerned about their online privacy compared to a year ago". People in the developed economies said they were losing their trust in the Internet because they are worried about "government behaviours and control by corporate elites". […] With greater amounts of data being collected about many more aspects of our lives, we will have even more to lose in future data breaches. If the burden of risk is not more widely shared — through clearer legal accountability and greater investments in security — the decline in overall trust will accelerate. [1]*

Having said this, it is clear that many citizens trade personal information for the services offered by platforms that are apparently free from the citizen's perspective. Studies have shown that social media users are much more interested in the services provided by the platforms than their own privacy concerns. Adams et al [12] sum up the situation:

> *Users will thus continue to be vulnerable to exploitation by companies like Facebook, who use their data for profit, as well as a wide range of services and technologies today that users are forfeiting their privacy to use many different services besides just Facebook. In the meantime, people around the world struggle to understand concepts like data ownership and informed consent for tracking cookies, so-called free email, and single sign-on services – and typically use the services regardless. [12]*

Users especially do not read the terms and conditions of platforms (which often change) – Obar et al [11] show that in an empirical study the vast majority of users ignore or quickly skim read the privacy policy and T&C of a fictitious social network, and conclude that information overload is a major negative factor. Comprehension is also a critical factor (see e.g. Reidenberg et al [13]) – many privacy policies are written in legal language and in such a way that their meaning can have numerous interpretations, so as to give the platform the maximum flexibility in utilising the information of its users. There is already work in the area of helping citizens comprehend the privacy policies of platforms, for example the H2020 SPECIAL project[9], and further work investigating comprehension issues needs to build on this.

Personal data spaces are a advocated as a mechanism to address the concern of privacy and support the owner's management of personal data (see e.g. [21]), and data market concepts are emerging where data can be traded for other items of value, but it is not clear how suited these concepts are for social networks, where users contribute information explicitly to share with friends, or to pursue a shared interest, and for this the social media platform is needed. Investigations are needed into how concepts such as personal data spaces and data markets that promote the control of data integrate with the critical mass of data needed to make social network platforms viable.

The trend towards personalisation is based on profiling, and a key feature of platforms' business models. There is a clear threat to privacy through the aggregation and profiling of platform users.

> *Personalization is also becoming increasingly important. Faced with content overload, consumers are supplied with recommendation systems designed to*

[8] https://www.vox.com/policy-and-politics/2018/3/21/17141428/cambridge-analytica-trump-russia-mueller
[9] https://www.specialprivacy.eu/



Co-funded by the Horizon 2020 Framework Programme of the European Union

> *help them select what they are going to watch or listen to. Automated processing based on artificial intelligence, algorithms and big data analytics is used to create tailored services, which are then pushed to mobile or web applications. Artificial intelligence's development is pervasive, including in the media arena, where it is already used to create news reports (notably on sport or stock exchange) and other media content. [7]*

Threats to data are not limited to personal data. Data is seen as a major commodity and source of wealth, and therefore is subject to threats to any other valued commodity (e.g. theft).

> *If "data is the new oil", the growing market for hacking and data theft puts the foundation of our future economy at risk. [1]*

Huge amounts of personal data are collected by Internet platform operators from the users of the platforms. The operators clearly consider this data a business asset, and users have little knowledge of what is being done with it. There is clearly a threat of privacy infringement or online surveillance through the analytics of the personal data. This threat is related to the dominance of large Internet corporations.

> *Some users already worry about the vast amounts of their personal data being collected and feel powerless to protect their personal privacy. Already, systems use data profiling to draw inferences about individual beliefs, preferences or habits in ways that are deeply personal. […] Advanced deployments of AI & IoT will result in the generation and collection of enormous amounts of information about individuals that can be analysed in ways that are deeply personal and that will raise the potential for a "surveillance society" to emerge. […] In some parts of the world, the Internet is being used as a tool for pervasive data collection, surveillance and control. [1]*

> *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. […] 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. […] Several long-term programmes for pervasive surveillance dating back to the earliest days of the internet have meanwhile been exposed, most notably [by] 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. [2]*

Interconnectedness and edge devices clearly have benefits, but there are also risks to both users and the infrastructure. Users are at risk of tracking, attacks and surveillance through security limitations of these devices.

> *A major security concern is the Internet of Things. This encompasses a proliferation of devices, whose security provenance and resilience may not be verified. Many IoT devices are created by manufacturers whose expertise lies*



Co-funded by the Horizon 2020 Framework Programme of the European Union

> *in areas other than Internet security, and devices may be infrequently or never patched to address security concerns. [3]*
>
> *If appropriate safeguards to ensure transparency and user control are not put in place IoT could drive data-collection and use in ways that further undermine privacy and deepen surveillance. [1]*

***Needs***

In summary, threats to personal freedoms and human rights are obviously paramount in the sources, and also in the HUB4NGI work, as these are pervasive themes. There is a need to address these aspects:

- Transparency of personal data processing, including where and how it is used in profiling of Internet users.
- Owner control of their personal data when used within Internet domains such as platforms, and how these concepts integrate with the critical mass of data needed to make social network platforms viable.
- Thefts and damage of citizens' data, irrespective of whether it is personal or not.
- Users' education regarding privacy and personal data, especially the unseen consequences of submitting information to (e.g. social media) platforms.

### 6.2.6 Limitations of Liberties

A significant threat is that governments, under pressure from national security threats, limit the personal freedoms of their citizens. Trading personal freedoms for national security is not a new theme (and varies from country to country), but new sources of threats are via the Internet itself (e.g. cyber-attacks), and the Internet is clearly a means of social utility that used properly can enhance freedom of expression. In a world of increased demands on national resources, accelerating cyber-attacks and ubiquitous connection to the Internet, there is a risk that personal freedoms enabled by the Internet especially are eroded (e.g. via censorship of Internet content or online surveillance) because of the need to address national security challenges, or national security is given as a pretext to justify liberty erosion.

> *The very tools that facilitate human empowerment can also be used to constrain it, and as the Internet becomes part of everything we do, the temptation for governments to use it to constrain will only grow. […] In such a world, the interests of national security will overshadow freedoms and rights. Whatever happens, we expect the tussle between perceived national security interests and end-user security measures (e.g., encryption) to continue. […] Efforts to develop online social norms or to address violent extremism online will challenge certain tenets of the Internet, namely, anonymity, privacy and free expression. […] But these Internet solutions may require tradeoff for Internet users. Anonymity and free expression may fall by the wayside in the drive to develop technology solutions and social norms to moderate online behaviour. [1]*
>
> *The trend towards interconnectedness poses threats, and that the ease of connectivity is a threat to countries' national security. [3]*

***Needs***

- Greater understanding of the Internet's impact on the debate concerning national security vs citizen liberty.
- Greater understanding of the Internet's impact on the debate concerning citizen free speech and censorship.



Co-funded by the Horizon 2020 Framework Programme of the European Union

### 6.2.7 Dominance of Large Corporations

Today, most peoples' experience of the Internet is via the channel or platform of a large corporation. There are a few that dominate the experience of Internet users and hold a great deal of information about these users. The situation is by and large monopolistic, as there is typically one dominant leader in each Internet sector (e.g. retail, search, social media, consumer hardware, etc), and this situation is far from the original ideal of the Internet as an egalitarian environment with equal opportunities for all. As with any monopoly, there are significant risks to society (and the economy) as the powerful corporations consolidate their power, such a lack of choice and intrusive & excessive controlling behaviour.

> *Consolidation of networks and platforms within a few organisations will affect the ability of networks to grow and scale and will limit the ability for new players to emerge. […] if the Internet platforms of today consolidate their power — becoming dominant across infrastructure, services and applications — user choice and control over their online experience, as well as the availability and diversity of information and content, could be constrained. […] Although there is a collective responsibility to ensure that the Internet is not used as a tool of control, much of the burden will fall on the shoulders of the companies running networks or platforms and manufacturing connected devices. How industry and particularly the Internet companies react to government pressure will help determine the future of the Internet as a space for free expression or for censorship and surveillance. [1]*
>
> *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. [2]*
>
> *The socioeconomic implications of a few large corporations holding monopolies. [3]*

There is a strong trend towards platforms as powerful content repositories and the source of the dominant Internet companies' revenues. Much of the content is user-generated, e.g. postings made on social media networks, and the key business model is that the content is used to target advertising. The platforms operate as a two-sided market: on the one side there are the users, who supply and consume content (usually free at the point of use), and on the other side there are the advertisers, who place advertisements that are targeted by the platform to relevant users. The advertisers are charged by the platform for the targeting service. Because they are operated by commercial concerns, these platforms are by nature silos, whose operators' main interest is keeping the content and using it for commercial purposes (such as targeted advertising). This pattern leads to fears of lock-in and monopolies, where users have no alternative but to use a platform because it is either the only option or the user's data is so deeply embedded.

> *The platformization of the digital European market raises various challenges as market power becomes more concentrated and a handful of stakeholders become the gatekeepers. Investment in technological innovation today in Europe is dwarfed by powerful global players. The European media research and innovation landscape is fragmented and lacks coordination. [7]*



Co-funded by the Horizon 2020
Framework Programme of the European Union

> *Market consolidation by Internet service and access providers could spur the growth of so-called "walled gardens" — closed platforms with proprietary ecosystems — leading to a loss of choice, constraints on innovation and Internet fragmentation. [1]*

Proprietary standards are reinforcing the position of dominance, and open standards are advocated as a response to the potential lock-ins associated with proprietary standards.

> *[…] developers are increasingly relying on proprietary standards which will be a barrier to innovation and interoperability. Open standards development will need to evolve to ensure standards are still relevant in a world of competing proprietary systems. [1]*

A key question is how long will the current form of platforms dominate? History has shown that dominant sectors of business changes over time – in a historical study over one century[10], the top 10 US companies in 1917, 1967, and 2017 are almost all different, although there is a clear trend towards technology over these three snapshots: in 1917, the top four were steel, telephony and oil, in 1967, the top four were computer manufacture, telephony, photography and automotive, and in 2017 the top four were all technology platforms: Apple, Alphabet (Google), Microsoft and Amazon, with Facebook fifth.

***Needs***

Investigations concerning the implications of monopolistic economies delivered over the Internet (for example the impact of platforms), the risks and inequalities these monopolies pose, and how the risks and inequalities may be addressed.

### 6.2.8 Threats to Employment

The automation brought about by Internet and related technology such as AI has brought with it fears that employment will be severely eroded by the automation.

> *As AI and automation drive significant structural change across industries, the very nature of work will change. Many existing jobs may be displaced as AI moves beyond monetising user data to changing how products and services are delivered. Adapting to the pace of change will be a major global challenge for the immediate future. [1]*

HUB4NGI work concurs with these points: the automation brought about by Internet and related technology such as AI has brought with it fears that employment will be severely eroded by the automation.

> *Wealth distribution models that accommodate humans and machines, so that the needs of both types are addressed. [3]*

***Needs***

Investigation into alternative employment creation and wealth distribution models is needed. Employment crises caused by automation are nothing new and historically society has recovered and eventually prospered, but transition periods are painful. The current situation is that we are in a transition period, reacting to the step change in communication and interconnectedness caused by the advent of the Internet, and society needs to understand how to navigate this transition to the maximum benefit for all and with as few casualties as possible.

[10] A Century of America's Top 10 Companies, in One Chart https://howmuch.net/articles/100-years-of-americas-top-10-companies



Co-funded by the Horizon 2020 Framework Programme of the European Union

### 6.2.9 Misinformation, Bias & Opinion Manipulation

The Internet is an open forum for myriad discussions and it has always been a key feature that there is a lot of incorrect information in its content. Propaganda has also been around for a long time, but current trends towards deliberate misinformation using the communicative power of the Internet as a channel to reach millions of citizens with a view to manipulating and perverting peoples' opinions is especially concerning in the light of social movements such as populism and nationalism aiming to undermine political systems such as democratic processes and established norms of power.

> *While democratising access to information, the whirlpool of information and misinformation that exists online is raising real concerns about the long-term effects of new trends such as fake news. […] Acts of cyber conflict will be coupled with disinformation and propaganda to destabilise states and economies. [1]*

There is a clear trend towards extremist organisations using the Internet as a communication channel, and the extremists are highly organised.

> *There is a tension between an open society and a closed society as espoused by extremists. The Internet is becoming a battleground for the larger societal ideas/tensions. The extremists have an online strategy — this should be paid attention to. There will be question around control and ethos of the Internet. Are there going to be new norms on the Ethos of the Internet and how does the political establishment view this? [1]*

Users are often unaware that the content they are seeing may be biased. A case in point is the so-called "search engine manipulation effect", where search results are tuned, prioritised and filtered based on algorithms only known to the search engine provider. There are clear relationships between this issue and the monopolies of large corporations and dominant platforms, and all contribute to a situation where the user does not know if they are receiving unbiased information.

> *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. [2]*

> *Beyond the problems that usually go hand in hand with a lack of competition in some activities, induced by oligopolies or quasi monopolies, there is a more general problem, which is a lack of transparency. Platforms use algorithms, e.g. to rank content, and this influences the way in which content is displayed for each user. As the recent cases of Facebook and Cambridge Analytica have shown, however, such algorithms lack transparency, for users as well as other stakeholders (e.g. the providers of the content that are then ranked). […] The role of platforms must doubtless be assessed. While most platforms do not have editorial responsibility over their content, some platforms (e.g. social media) play a key role by influencing the display of content, or more broadly, the way content is presented to the public. For search engines, search results should objectively reflect the search request, without undue commercial influence on these results. Search results should equally not privilege those services owned, administered or controlled in whole or in part by search engines. [7]*



Co-funded by the Horizon 2020
Framework Programme of the European Union

Citizens may be unaware that they are receiving filtered and personalised content. The result is that they experience the so-called "filter bubble", where their opinions and preferences are reinforced through a lack of diversity of opinion.

> *Regarding the impact of personalization, there is a risk of filter bubbles developing, that is to say situations where users do not obtain access to and, hence, remain unaware about some types of content. Data driven and fully automated personalization models are not sufficiently looking into how to include diversity and serendipity in algorithmic functions to broaden the consumer's experience. [7]*

In addition to the providers filtering information, human interactions over the Internet can also result in a lack of diverse opinions, where citizens experience an "echo chamber" of their own opinions. The Ditchley Foundation consultation states that:

> *[…] there is a risk that the Internet becomes an echo chamber for our own prejudices and preconceptions, rather than a source of objective facts and challenge. [8]*

***Needs***

These phenomena threaten society in that they can lead to polarisation, ignorance, intolerance and extremism. In some cases, these phenomena are tools used by individuals or organisations that wish to convert opinions towards their cause. In other cases, they are communication mechanisms or socio-technical structures where opinions are polarised (either unknowingly or knowingly) based on the interest of the participants in either confirming or correcting biases. Clearly, work is needed to address these phenomena: misinformation needs to be identified and exposed as fake, how the Internet is used by extremist organisations needs to be understood, investigations and experiments to understand the filtration of Internet content based on profiling are needed to further understand the phenomena, and the dynamics of different kinds of echo chambers needs to be studied.

The needs from the external sources above concur with the recommendations from the HUB4NGI consultation with domain experts on the related subjects of fake news, echo chambers and populism [5]. Its key overarching recommendation is that **we need to understand how opinions are formed and are influenced in the current digital age.** Investigations are needed to understand the underlying cognitive and emotional processes that enable peoples' opinions to be influenced in the context of a ***hybrid media system*** following Andrew Chadwick's work[11] that mixes online and offline channels and broadcast and interactive social media.

- ***Fake News.*** Understanding the societal effects of fake news is important – whether people believe it, whether and how they distribute it and whether they are influenced by it. Investigation of effective and observable measures for the influence of fake news is advocated. Effective mechanisms are needed to address three specific elements of fake news: *emergence*, *distribution* and *effects*. The propagation of fake news needs to be studied, especially within and across hybrid media systems. Fake news propagation patterns, strategies and effects need to be evaluated in different countries and world regions. We need to understand how the new dissemination channels offered by the Internet and social media contribute to the social effects of fake news and propaganda. Understanding of the different actor types who spread fake news is needed, coupled with their motivations for doing so.
- ***Populism.*** There is a need to investigate the root causes, underlying forces, evolution, and dynamics of different types of populism. We need to understand how people are socialised into populist movements. The phenomenon of populism is well studied, but

[11] Chadwick, A., 2017. *The hybrid media system: Politics and power*. Oxford University Press.



Co-funded by the Horizon 2020 Framework Programme of the European Union

we specifically need to understand the contribution of hybrid media systems including interactive online communities, plus fake news and echo chambers' contributions to populist recruitment; individually and in conjunction. Investigation into measures to address populism is recommended. A specific point made by the panel is to understand and assess the effectiveness of the different countermeasures currently employed by different societal actor types to address populist activity, and to learn from them.

- ***Echo Chambers.*** Investigation is needed to characterise echo chambers to: describe them, to find out how they are working and understand how effective they are at reinforcing entrenched beliefs. We need to understand how echo chambers are supported by hybrid media systems. We need to investigate how selective filtration and suggestion by search engine providers influence polarisation. Research is needed to determine distinctions and interplay between confirmation bias and critical analysis. What characterises the situations and people that determine whether confirmation bias or critical analysis takes precedence? Motivations for people joining, participating in, staying and leaving echo chambers need to be investigated.
- ***Research.*** Understanding how to assess the veracity of information is needed. Specifically needed is to understand how people (of different types, e.g. professionals, private citizens and others) assess the truth in a piece of information is needed, as well as how to help people assess the truth of a news item. Exploration of diversity in terms of the information sources that people see is needed so that people get the option of exposure to diverse viewpoints, but this should be investigated considering the motivations that determine whether people will read them. We need to guard against partisanship or inherent bias in potential solutions. Collaborative, interdisciplinary research is needed, and cross-discipline collaboration needs to be improved. Funding is needed to enable this interdisciplinary collaboration. A diverse population of subjects for interviews and experiments is needed, and trust of the target community is essential in an experiment study. In addition to standard data gathering methods such as surveys or interviews, methods specifically observing peoples' response to fake news are needed. Multiple research approaches and mixed-methods research are advocated to cross-check and validate evidence generated through different methods. Skills needed to address the inter-related challenges of fake news, echo chambers and populism include: social science, ethnography, data gathering, qualitative and quantitative analysis, statistics; and hypothesis development coupled with experiment design. Definitions and conceptual models for key terms are needed, with the caveat that while there is a need for adequate definitions, exhaustive, full-consensus definitions are likely to be difficult and unnecessary. We also need to acknowledge that there may be different definitions for the same term or concept and to understand the effects of using different definitions. New and diverse datasets are needed – there is too much reliance on existing benchmark datasets. Funding is needed for the purchase (or collection and cleaning) of large new data sets. Social media data is especially needed, and it is recommended that social media operators be encouraged to make it easier to access their data. The current situation is that it is very difficult, and in some cases impossible, to access this data, which is a major barrier to quantitative research and analysis. A directory of existing tools and methods is proposed, that can act as a one-stop-shop so that researchers (and citizens) can access them and can understand what resources are available.
- ***Societal Impacts.*** We need to test the overall hypothesis that fake news, echo chambers and populism have detrimental or destabilising effects on democracy. We need to understand each of their individual contributions, as well as their effects in combination, to the undermining of liberal democracy. Individual and collective effects of fake news, echo chambers and populism on citizens need to be investigated. What factors determine citizens' susceptibility, and what makes some citizens more susceptible than others? Secondly, we need to understand the effects on "bystanders" – citizens who see fake news or populist content etc, but do not actively engage with it.



Co-funded by the Horizon 2020
Framework Programme of the European Union

In addition to fake news and echo chambers, the social influences of search engine manipulation, search result filtration and search suggestion mechanisms need to be investigated.

## 6.3 APPENDIX 3: GAP ANALYSIS OF CURRENT NGI WORK PROGRAMME

This section provides a discussion of the current NGI work programme [18] in terms of an analysis of gaps between the threats and needs identified in the previous sections and what is already in the work programme. Each element of the NGI programme is discussed, but some are more relevant to the subjects identified in the previous sections than others, and this is highlighted. The results of this gap analysis will feed into the recommendations in the Roadmap section.

### 6.3.1 ICT-24-2018-2019: Next Generation Internet - An Open Internet Initiative

This is a program of thematically-organised projects that utilise cascade funding via open calls supporting “advanced research that is linked to relevant use cases and that can be brought quickly to the market”. Third parties can apply for cascade funding amounts between EUR 50K and EUR 200K for small close-to-market research projects lasting up to 1 year. The subjects for the first two phases are as follows.

- Open Calls Commencing Q4 2018
    - Privacy and Trust Enhancing Technologies
        - Sensors, devices, AI-based algorithms incorporated in our digital environment
        - Greater control when sharing personal data, attributes and information
        - Robust and easy to use technologies
    - Decentralised Data Governance
        - Open hardware and software ecosystems based on blockchains, DLT, P2P technologies
        - Attention to ethical, legal and privacy issues
        - Supporting autonomy, data sovereignty and ownership
    - Discovery and Identification Technologies
        - Large heterogeneous data sources, services, objects and sensors, multi-media content
        - Contextual querying, personalised information retrieval and increased quality of experience
- Open Calls Commencing Q4 2019 or Q1 2020
    - Strengthening internet trustworthiness with electronic identities
        - Authentication, authorisation, traceability, privacy and confidentiality (incl. objects, …).
        - New business models for verifying and evaluating data
        - Scalability, standardisation, deployability, ease of use
    - Service and data portability
        - Separation of data from services provided to end-users



Co-funded by the Horizon 2020 Framework Programme of the European Union

        - Handling mixed data sets, standardisation, operational and business models
        - Techno-legal constraints, simplification of terms of use
    - Open internet architecture renovation
        - Internet architecture evolution towards better efficiency, scalability, security & resilience
        - Auditing, testing and improving protocols and open source SW and HW
        - Ability to roll-out at internet scale

Many of the subjects covered here have been highlighted by the external sources and in the HUB4NGI studies, but they cannot be sufficiently addressed by small close-to-market projects alone, so it is recommended that some subjects are investigated at the in-depth research level, as well as at close-to-market level.

- The theme of "trust" is a vast, multifaceted subject that has been discussed in Section 6.2.1, where it is asserted that public trust is declining in the Internet. Indeed, any perceived threat has significant potential to reduce levels of trust, so most of Section 6.2 is relevant to the theme of trustworthiness in the Internet. Specific examples include Section 6.2.4 concerning the specific case of trustworthy AI and Section 6.2.9 covering the manipulation of citizens' opinions using (amongst others) Internet channels. Therefore, the theme of trust cuts across many other subjects and requires multiple strands of coordinated and in-depth research to address the challenge sufficiently. Some of this work can be within the NGI, but others (in particular cyber security) are covered in other focus areas, so it is likely that coordination across these focus areas will be necessary.
- Renovating the internet architecture addresses key threats identified in Section 6.2.2, but addressing these challenges will require a huge effort and collaboration on a global scale. Standardisation will be a key factor for interoperability and understanding, and an endeavour of this magnitude and fundamental nature needs to be open, multi-stakeholder and multi-national so as to avoid any partisan or proprietary commercial or national bias or advantage. In addition to determining new standards and re-engineering the Internet stack, enabling seamless transition from existing stack technologies is necessary so that there are no service interruptions. Clearly, small, close-to-market open calls are not adequate to address this challenge.
- Data sovereignty, i.e. owner-control of personal data and full control over data sharing is mentioned in multiple subsections of the ICT-24 topic, within "Privacy and Trust Enhancing Technologies", "Decentralised Data Governance" and "Service and data portability". The issues surrounding these issues need further in-depth research and given that data sovereignty is a major theme that concerns the users of the Internet, for example privacy violations contribute to a decline of trust in the Internet (discussed in Section 6.2.1), and also violate personal freedoms and rights (discussed in Section 6.2.5), it is suggested that data sovereignty have a topic in its own right.
- The "Discovery and Identification Technologies" theme covers advanced search topics, but does not cover the challenge of search engines filtering content based on profiling of Internet users.

### 6.3.2 ICT-25-2018-2020: Interactive Technologies

This call covers augmented reality & virtual reality: subjects have not arisen in the work of HUN4NGI, nor in the external source analysis. Therefore, there is no comment on these subjects.



Co-funded by the Horizon 2020 Framework Programme of the European Union

### 6.3.3 ICT-26-2018-2020: Artificial Intelligence

This call covers the need for an “AI Platform”, a one-stop shop where AI, its applications and the so-called “ELSE” (Ethical, Legal, Social, Economic) aspects are brought together, so that the AI technology may be more widely used to greater advantage than previously. One call was launched in 2018, and a second is planned for 2020.

There is clear cross-over here with the Responsible AI consultation. The call mentions determination of a strategic research agenda for AI, specifically including ELSE aspects, but does not cover the following aspects, which are recommended by the Responsible AI consultation.

- Trustworthiness of an AI system is critical for its widespread acceptance, so understanding the factors that contribute to a trustworthy AI system is also critical.
- The need for transparency in AI reasoning and provenance of training data. It is advocated that a library of training data, annotated with provenance information be built, which is publicly accessible to benefit other users apart from its creator.
- The need for case studies to investigate the implications of different AI application cases. The scope of the analysis in the case studies covers ELSE plus other aspects: it is advocated that ethical considerations; responsibility & accountability; relevant regulations & legislation; monitoring of behaviour; and failures & remediation are covered.
- Investigation of the socioeconomic impacts of AI & autonomous machines on society, especially how AI automation differs from other types of disruptive mechanisation. This especially includes AI’s impact on human workers – how any threats or negative effects such as redundancy or deskilling can be addressed.

### 6.3.4 ICT-27-2018-2020: Internet of Things

This is a coordination and support action to determine future research and policy in the domain of IoT. There is a clear link to the IoT security requirements mentioned in Section 6.2.2, but the challenges of IoT weaknesses and protection from attacks will most likely require full research topics to ensure that they are adequately covered: most likely the threats to IoT devices need to be monitored continuously and addressed within research projects.

### 6.3.5 ICT-28-2018: Future Hyper-connected Sociality

This is a wide-scope topic that covers a number of themes highlighted in this deliverable, most notably owner-control of data when processed at third parties (discussed in Section 6.2.5), dominance of large platforms discussed in Section 6.2.7) and verification of content in order to address misinformation (discussed in Section 6.2.9).

ICT-28 contains an Innovation Action covering content verification in social media, and this clearly crosses over with the fake news aspect of the Opinion Forming consultation. However, the Innovation Action covers just social media and a key recommendation of the Opinion Forming consultation is that misinformation propagates over a hybrid media system, with different kinds of media (online, offline, broadcast and social media) interacting as necessary, so there is a need for expanding the scope of the misinformation to include other media types.

ICT-28 has a second Innovation Action covering business models, governance and proofs-of-concept for secure and fair sharing of data. A key aspect that is missing is examination of the vested interests of the parties and how this affects the risk levels of the owner of the data. Another aspect that should be considered is how these models and structures affect the dominant platforms, who are likely to see no reason to move to new models, and so investigations into how to incentivise the dominant platforms into participating in these models is needed.



Co-funded by the Horizon 2020
Framework Programme of the European Union

ICT-28 contains one Research and Innovation Action covering investigations into decentralised and distributed social networks, as an alternative to the current monolithic incumbent platforms. As with the previous comment, there is a need to investigate how these new architectures will affect the current incumbents, but also how users can be encouraged to migrate to these new social network architectures, especially when the dominance of the current incumbents is founded upon a critical mass that they have already achieved. How can any new entrants compete?

ICT-28 also contains one Coordination and Support Action aimed at promoting community building between multi-disciplinary researchers, industry and other interested parties to enable cross-disciplinary collaboration in the creation of new patterns for social networks. This clearly is in line with the key observation that multidisciplinary collaboration (Section 6.4.1) is critical for much future NGI development.

### 6.3.6 ICT-29-2018: A Multilingual Next Generation Internet

This call covers the need for addressing the barriers of Internet content written in different languages. Whilst they are clearly important, these topics have not arisen in the studies conducted by HUB4NGI, so no comment will be made.

### 6.3.7 ICT-30-2019-2020: An empowering, inclusive Next Generation Internet

This topic covers the support of equal opportunities through education for all - personalised learning, so as to enable all kinds of Internet user to benefit fully from the interactions via the channels and platforms provided by the Internet. The structure of the projects funded under this topic uses cascade funded open calls to enable addressing specific challenges. A key challenge not mentioned is the need to understand how to provide education to enable Internet users to make informed judgements about the risks and threats of Internet locations and content (discussed in Section 6.2.2 within the context of cyber threats). A further challenge not mentioned is the need for a flexible workforce to address ever-evolving technological developments in automation with associated threats of human redundancy (in particular from AI research), discussed in Section 6.2.8, so understanding how to educate a workforce of citizens so that it is sufficiently adaptable to changing employment needs is needed.

### 6.3.8 ICT-31-2018-2019: EU-US collaboration on NGI

This topic covers facilitating collaboration between the EU and the USA on NGI topics. The mechanisms are via events, workshops and exchange programmes, plus a Research and Innovation Action operating cascade funding open calls for collaborative EU-US experiments in NGI topics. A key topic that would be a good candidate for EU-US collaboration is the need for Internet infrastructure renovation discussed above as part of Section 6.3.1, because inter-continental collaboration is needed in order for any changes in the Internet stack to be widely adopted.

### 6.3.9 Other Areas of the Work Programme

The analysis presented in this document covers areas of the work programme that are not within the NGI specific topic. The primary areas are described as follows. They are outside the scope of the NGI, so detailed analysis has not been performed, but general comments are made.

- *14. Secure societies - Protecting freedom and security of Europe and its citizens* [19]. The discussion in Section 6.2.2 clearly highlights the need to continue investment in cyber security, because the attackers will not stand still, and so the defences need to keep pace: new threats will continually emerge, and constant vigilance to identify new threats is required. The current foci highlighted in Section 6.2.2 are defence against attacks on critical infrastructures (covered in SU-INFRA01), destabilisation of



Co-funded by the Horizon 2020 Framework Programme of the European Union

governance and political systems (covered in the counterterrorism topics SU-FCT01 to SU-FCT04 inclusive), investigating the threats and weaknesses of IoT devices (not covered) and addressing weaknesses in lower layers of the Internet (not covered), so if recommendations for the Secure Societies call are required, they would be to include investigations into IoT threats and to address the weaknesses of the lower layers of the Internet technology stack. For both of these areas, discussions would be required to determine where support for such work would be best located, as they could equally fit within cyber security or the NGI.

- *13. Europe in a changing world – Inclusive, innovative and reflective societies* [20]. There are many societal impacts discussed in previous sections, for example public trust in the Internet (Sections 6.2.1), digital divides (Section 6.2.3), personal freedoms & rights (Section 6.2.5), threats to employment (Section 6.2.8) and opinion perversion (Section 6.2.9). These areas are primarily concerned with the Internet's impact of public life, and so addressing them is most likely best included within the NGI programme, but there may be specific areas that are more suited to the Societies topic, so collaboration between the organisers of the NGI and the Societies programmes is recommended, so as to come to an agreement as regards the most useful division.

## 6.4 APPENDIX 4: NGI PROGRAMME IMPLEMENTATION AND COMMIUNITY SUPPORT

This section summarises work done in other HUB4NGI work packages and contains practical experiences, observations and recommendations for implementing the NGI programme.

### 6.4.1 Multidisciplinary Collaboration

Collaboration between different disciplines is seen as necessary to find solutions to Internet challenges. A particular case for multidisciplinary collaboration is defence against cyber-attacks.

> *The complexity and scope of cyberattacks necessitates multistakeholder and expertise driven responses for the digital economy to thrive and for trust in the Internet to be rebuilt. […] If, when faced with cyber threats, stakeholders respond constructively with coordinated responses to cyber incidents, mutual cooperation on cybercrime, convening multistakeholder platforms to better collaborate on national cybersecurity strategies, and ensuring respect for human rights, then cyber risks can be better managed and mitigated, and trust restored. [1]*

***Needs***

As a general rule, collaboration between different disciplines, especially between socioeconomic, legal, ethical and technology should be enabled and encouraged in order to understand the ELSE (ethical, legal, social and economic) aspects of Internet technological developments, and thence to create human-centric Internet technologies & protocols.

Collaboration between different disciplines is seen as necessary to find solutions to Internet challenges. This reflects the intersection between technical developments in the Internet and the Internet's social impact, and may involves technology, hard science, soft science, commerce, law and government.

> *Multidisciplinary Design is viewed as important by almost all of the sources surveyed, and involves bringing together the right mix of experts from different disciplines who collaborate to address the problem at hand. In particular,*



Co-funded by the Horizon 2020 Framework Programme of the European Union

> *multidisciplinary teams are deemed particularly necessary when deciding on governance or legislation over Internet technology and applications. [3]*
>
> *[EC support is essential for] Collaboration and finding new partners and stakeholders (51% of respondents) [HUB4NGI Survey]*

The NGI Survey found that collaboration between different types of participant is also helpful in addressing the challenges of the NGI, as well as providing means for small organisations (e.g. SMEs) to participate in collaborative research and innovation.

> *EC support is therefore particularly valuable to support innovation and knowledge sharing as well as for creating networking opportunities which are important specially to support small companies (which made up the 94% of the technology providers sample) [HUB4NGI Survey]*

In addition, the NGI Survey found that supporting large scale experimentation facilities is valuable as they provide resources not usually available to small organisations and are necessary for testing ideas at scale and in realistic environments.

> *Furthermore, what emerged as relevant for the future of internet is keeping focusing on large experimentation and testing in a semi-real environment as this is crucial to ensure commercial success of new products and to bridge the gap between market and research. [HUB4NGI Survey]*

Supporting collaboration via innovation hubs and other mechanisms that bring people together is seen as strongly beneficial. As illustrated in Section 6.4.4, the NGI Community Map identifies potential collaboration partners via physical geography and similarity of subject area and organisation type, which supports the Innovation Pathways work described in D2.2 and D3.2. The map also highlights geographical clusters of NGI innovators, which may be candidates for forming local innovation hub, if it does not exist already.

### 6.4.2 Assessing the Effectiveness of the NGI

HUB4NGI WP1 has contributed two aspects to measuring the effectiveness of the NGI programme. They are:

- Key Performance Indicators in different groups, to provide measurable assessment of different aspects of performance; and
- A survey of NGI initiatives, participants and users, to gather opinions on the effectiveness of the NGI programme from different perspectives. This has resulted in key recommendations, summarised in this section.

#### 6.4.2.1 Key Performance Indicators

The KPIs framework developed is described in detail in D1.1, D1.2 and D1.3, and focuses on the following indicators:

- Innovation → measuring the degree of innovativeness of the identified NGI initiatives, including similarity with other solutions already available on the market, type of innovation (incremental vs radical), if a solution has been described in trade or scientific publications, how near a solution is to be commercially exploitable, and if a solution is a stand-alone or part of a larger organizational technology development roadmap.
- Sustainability → quantifying how much external funding is needed to develop the solution before reaching economic sustainability.
- Collaboration → assessing if the identified NGI initiatives are adopting open innovation models collaborating with external partners for the development of the solution



Co-funded by the Horizon 2020 Framework Programme of the European Union

- Openness and Use of Standards → measuring how well do the NGI initiatives contribute to the existing framework of open source development and adoption of technology standards.
- Market Needs → assessing if NGI initiatives are able with their solutions to fulfil the most important needs of the targeted vertical markets.
- Social Utility → this KPI quantifies the ability of an initiative to address key issues related to European societies. This allowed to identify which societal challenges a solution contribute to, including the overall fitness of the European citizens, the overall health of the European population, clean, efficient, sustainable energy, public transportation challenges, the reduction of waste of finite resources, speed of communication and the ubiquity of connection, inclusion, collaboration, protection from attacks such as cyberterrorism, identity theft, fraud, cybercrime and cyberbullying, e-learning, perceived security of communities, neighborhoods, and housing, and access to relevant information.
- User experience → defining the ability of initiatives to put users at the center of their strategies, considering users' satisfaction, ease of use, development of new skills, customization, collaboration and potential risks.

#### 6.4.2.2 Survey Methodology & Results Summary

This chapter contains some insights into the performance assessment carried out within Next Generation Internet (NGI) initiative, to assess the success of NGI initiatives as well as the broader value generated by European Commission support. Full details are found in D1.3 [9], but a summary is presented here.

HUB4NGI, carried out between September and November 2018, a survey titled SURVEY4NGI, focused on assessing how well NGI initiatives respond to NGI objectives as well as European Commission's effectiveness in supporting innovation in Europe, major gaps and future areas of research. The sample of the survey, consisted of 63 respondents, made up of technology providers, research projects and policy makers or initiatives funding 3rd parties.

The survey analysed NGI initiatives with respect to the Key Performance Indicators, which include Innovation, Sustainability, Collaboration, Interoperability, Market Needs, Social Impact and User Experience. Results highlighted that collaboration and user experience are the areas where NGI initiatives are stronger, while areas of improvements include interoperability (through extensive use of open source instruments and standards) and innovation.

SURVEY4NGI besides assessing NGI initiatives' maturity and effectiveness also provides the European Commission with some valuable insights to better understand its role in supporting European initiatives and identifies those areas where this support could improve, drawing a roadmap for future development and activities.

Regarding the impact and value generated by EC, the survey investigated the following:

- Direct/indirect value perceived by initiatives supported by EC and potential values expected by initiatives that have never been involved in EC projects
- Major areas of improvements and additional support that EC can provide to foster European innovation
- Future technological areas that EC can support in the future



Co-funded by the Horizon 2020 Framework Programme of the European Union

As the main benefits perceived from EC support is concerned, the top three benefits selected by NGI initiatives[12] are:

1. Developing new ideas and products (60% of respondents)
2. Collaboration and finding new partners and stakeholders (51% of respondents)
3. Gaining new knowledge (45% of respondents)

EC support is therefore particularly valuable to support innovation and knowledge sharing as well as for creating networking opportunities which are important specially to support small companies (which made up the 94% of the technology providers sample)

The top three areas of where EC interventions are most appreciated are the following:

1. Funding availability (51% of respondents)
2. Reaching the target market (40% of respondents)
3. Project visibility (38% of respondents)

The major areas were EC can focus on to better foster a European innovative ecosystem is therefore increasing market support to innovative companies, enabling them to reach their target markets and commercialize their innovations while improving companies' visibility with respect to both potential customers and investors. Facilitating access to funding programs and participation from start-ups is another area where there is space for improvement, according to respondents' feedbacks.

The NGI Survey has highlighted that industry-specific programs (for example targeting creative industries, bioengineering and energy sectors) are useful to their target audience and warrant sustaining. Furthermore, continued support of large-scale facilities for experimentation and testing in a semi-real environment is recommended as this is crucial to ensure commercial success of new products and to bridge the gap between market and research.

To explore the spectrum of future trends, most initiatives mentioned Artificial Intelligence, 5G, security, IoT and Edge/Fog Computing as topics to be further supported in the future. Industry specific programs were listed as worth to be further sustained, for example creative industries, bioengineering and energy sectors.

Key **recommendations** for future NGI activities can be summarised as follows:

- **Foster NGI initiatives' go-to-market effectiveness**: One of the key needs for NGI initiatives, especially for those technology and solution providers at their early business stage, is a further support in go-to-market activities and sales effectiveness, helping start-ups and SMEs move from a fully-funded projects status to solid commercial entities. This translates into multiple best practices, ranging from the organisation of technology industry-specific end-users-oriented events that could facilitate an interaction with targeted industries, to marketing support both in terms of market visibility enablement activities and customer needs understanding, and to support in cross-countries activities, opening initiatives' addressable market to broader scenarios.
- **Support innovation development and scalability:** Another important area where EC support can improve is the provision of shared infrastructures, tools and data that can be leveraged by innovative companies, especially SMEs, in order to validate their technologies and turn their proofs of concept into market ready products. Sharing infrastructures and tools can help these companies to cut down their fixed costs and develop their innovations rapidly. Fostering scalability, reliability and interoperability is

[12] Sample includes policy makers or initiatives funding 3rd parties, research projects that have been receiving funds form EC, and technology providers that have been involved at least once in a EC funded project (N=55).
Source: HUB4NGI, November 2018



Co-funded by the Horizon 2020
Framework Programme of the European Union

the following step for ensuring technology development and this is another aspect where EC can reinforce its actions. Promoting a trustworthy environment where technology standards and open source models help build on each other progresses in a cumulative way is a win-win approach that the EC should encourage more in the future.

- **Help different industries and projects speak to each other**: The importance of a solid partners ecosystem is clear among NGI initiatives. The efforts put in place by the European Commission to foster the creation of new partnerships and networks among technology providers, end-user communities and public institutions in recent years have been massive and their effectiveness is recognized when also speaking with NGI initiatives. The further step towards a holistic partner ecosystem paradigm is now the creation of connections between different and potentially far domains and industries, fostering knowledge and information sharing, while creating the basis for synergies and complementarities between different sectors. This not only means having the different cascade funding projects sharing ideas and approaches, but also facilitating the interaction between companies targeting different industries and with separate product/service portfolio. A cross-fertilization between industries and technology domains, could enable innovative ideas and unexpected technology applications and use cases, while opening new business opportunities.
- **Keep pushing sustainable development**: There is considerable evidence that governments are under significant pressure from multiple factors, including increasing urbanization, an ageing population, waste of finite resources, growing inequalities etc. New technologies are increasingly playing an important role in addressing several of these societal challenges. The European Commission has already fully embraced and actively committed to the 2030 Agenda and the 17 sustainable development goals launched by the UN. However, the journey towards a sustainable Europe is only at the beginning, continuing supporting this vision with dedicated actions and specific innovation programmes is essential to progress along this way.
- **Expand existing technology focus towards promising emerging themes**:
    - **Further sustaining these technologies**. Technologies such as IoT, Artificial Intelligence, 5G, Cybersecurity/Privacy and Open Data were highly recommended by the surveyed NGI initiatives as those areas where EC activities should focus more in the future. This highlights how these technologies, already in the NGI scope, are extremely valuable for EU organisations. Recommendation for EC is to keep expanding research and innovation in these areas, with a focus on the less developed use cases such as self-driving vehicles.
    - **Do not forget established technologies**. Medium relevance resulted for more established technologies such as big data, visualization tools, cloud, intellectual property and digital copyright and e-learning. Most of these technologies represent key enablers for emerging technologies development. This suggests to EC that keeping an eye on the enabling infrastructure and tools is important.
    - **Keep scanning the horizon**. Other emerging topics and technologies were mentioned by NGI initiatives as possible areas that EC should take care of in the future. Some of these emerging trends are edge computing, digital fight to fake news, personal data digital twins, neuromorphic computing, quantum computing, and bio-engineering. Furthermore, what emerged as crucial particularly for these emerging topics is keeping focusing on large experimentation and testing in a semi-real environment to ensure commercial success of new products and bridge the gap between market and research.



Co-funded by the Horizon 2020
Framework Programme of the European Union

### 6.4.3 Open Call Management

The work in HUB4NGI WP3 has discussed experiences and recommendations for management of Open Calls to support innovation and experimentation using the EC's Cascade Granting mechanisms. Details can be found in D3.2 [10]. D3.2 lists the recommendations for supporting Open Calls in detail by describing different types of Open Call and provides suggested templates for key documentation such as application forms, agreements and policies.

During the course of the project different types and formats of Open Calls have been set up and feedback on this process has been collected from the participating parties. The main conclusions from these experiments are:

- Setting up Open Calls, includes decisions on the format of the Open Calls. These formats can be standard formats, thematic calls, continuous calls, calls targeting specific classes of proposers. The choice of the format clearly links to the scope of the call and the targeted participating parties.
- Running Open Calls includes the process of reception of the proposals, the subsequent review process and the follow-up and collection of results of the submitted projects. The use of external reviewers to review the submitted proposals is highly recommended to ensure neutrality and avoiding any conflict of interest.
- During the preparation of the proposals it is strongly advised, especially in Open Calls involving experimentation, to establish contact between the proposing parties and the owners and operators of the testbed and experimentation facilities which will be used. Involvement of the operators of the facility ensures the feasibility and compatibility of the proposal to run on the facility. This avoids possible technological roadblocks in the case the proposal is accepted for funding.
- During the experimental work and after the completion of the funded project, collection of feedback is necessary, not only feedback from the participation partner, but also form the facility operator. This feedback is important to tune future Open Calls, to address now topics through thematic Open Calls, identify existing gaps, …
- The administrative load to both the proposing party as well as the consortium running the Open Calls should be kept minimal. Especially when SMEs are targeted, it is essential to run a lightweight and fast decision-response mechanism. Such a process enables fast-moving organisations such as SMEs to access funding, whilst still ensuring rigour to justify the spending of public funds.

### 6.4.4 NGI Community Map: Stakeholder Analysis as a Contributor to Driving Innovation

Among the key resources identified as critical to the development of innovation pathways are:

- *Human geography*, in terms of physical closeness, of knowledge and other resources. The first, and most obvious, benefit of the NGI community map is the identification of potential collaborators or other stakeholders within a geographical distance.
- *Markets:* selected actors on the map serve as a component of the *market* that contributes to identifying innovative ideas and solutions, and the operational environment within which innovation is consumed or rejected. The map provides filters for organisation types - of interest here would be SMEs, start-ups, corporates and NGOs, as well as the governmental bodies (including policy-makers) who monitor impact of innovation on society and formulate or modify regulations as required to steer responsible application of technology.

A key resource in the definition of innovation pathways and conversion to actual innovation is knowledge, including topic and domain expertise. The breadth of expertise and experience across actors on the NGI map may be tapped into to support innovation. To support extraction



Co-funded by the Horizon 2020
Framework Programme of the European Union

and reuse of this knowledge, basic content analysis was carried out on the public descriptions actors provide.

This section illustrates potential to add value by extending the visual resource provided by the map in this way.

### Identifying Knowledge, Expertise, Gaps and Target Markets

To illustrate potential to extract value from the community map, the nine technology focus areas identified in D2.1 are used as a base to identify stakeholders on the map with expertise specific to the NGI aims, along with other related technology and expertise areas. The latter should aid also in identifying gaps within the innovation space. Actors on the map are either key drivers of or contribute to the conversion of innovation to practical application. The stakeholder analysis also looks at consumers of innovation, those actors whose work includes the identification of technology markets and/or are themselves a part of the target market. Interests and expertise in common may also be used to infer similarity between organisations and, therefore, potential for collaboration along innovation pathways.

Each actor on the map provides a brief description that includes their interests, expertise, examples of work or achievements and aims. Text mining allows the extraction of terms across all descriptions, to identify technologies and application areas mentioned by each actor and those in common across the database and subsets of actors. We employ commonality and frequency of terms to determine expertise within the community and similarity between actors.

It should be noted that relying mainly on automated text mining, the analysis is limited by small dataset size. It is therefore complemented by statistical analysis, where appropriate.[13] This limitation is countered also by manual inspection of selected data samples, to verify the results obtained. This has shown a good degree of reliability of the results. While too small a sample to claim definitive results, the content analysis exercise provides an initial filter that points to actors, as stakeholders, and areas of interest to explore further, to support innovation in the domain areas of particular interest to the NGI.

Supporting innovation pathways requires, first, the identification of technology areas/domains of interest to R&D and with clear and useful application to research, industry or that serves other public interest, along with corresponding expertise. Engagement with target markets willing to consume said innovation is essential; the alternative is risk expending effort and other resources in developing products and services that are ultimately rejected by the market. This section looks at two technology areas and a vertical sector in which both may be applied, to illustrate how the NGI community map may provide support for innovation pathways within and beyond the initiative.

### NGI Topic Artificial Intelligence

*Artificial Intelligence* (AI) is one of the nine NGI key topics, and also a topic of on-going popular interest. AI was one of the topics examined in HUB4NGI Deliverable D2.2, with respect to autonomous machines.

By filtering the data collected from the map to look at the nine NGI topics we can focus on those actors with interest and expertise in these topics, and by extension to other areas of interest. Table 2 shows the six actors who specify an interest and/or expertise in AI, along with a selection of other areas of interest addressed by these actors (see also the topic/knowledge network[14] in Figure 7). Three of these actors are startups/SMEs (su, sme in the table) and the fourth a business cluster (also NGI Contact Point – ngicp); some focus is expected on application markets, among those mentioned are *behavioral*, *healthcare*, *advertising* and *automotive*.

[13] Basic statistics on NGI map data content can be found in the Appendix in Section 6.4.4.1.
[14] Running automatically, some terms in the graph are essentially stopwords, e.g., *full*, *good*. *Big* may be a stopword or used in, e.g., "*big data*". Additional rounds of data cleaning are required to reduce stopwords to a minimum. Note also stemming is carried out to aggregate various forms of terms with essentially the same meaning - the most prevalent form of each stem is used in this document for readability.



Co-funded by the Horizon 2020
Framework Programme of the European Union

It should be noted that term frequencies are relatively low; this is however because the descriptions are generally very short, so that relative importance of mention is higher than expected.

Table 2: Actors specifying *artificial intelligence* in descriptions

| | type | artificial intelligence | data | secure | smart | market | behavioral | healthcare | advertising | automotive |
|---|---|---|---|---|---|---|---|---|---|---|
| DFKI | rc | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Cap Digital | ngicp | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 |
| MASA Group | sme | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 |
| nViso SA | su | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 |
| INOV-INESC Inovacao | rc | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| Perspect IT | su | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Table 2 is centred on AI, linked to the top 15 co-occurring terms and the next set of terms these co-occur with. Links coloured in orange note significance of the link between term pairs.

While connectivity to most of the first generation of nodes is obvious, the second generation is where related, but not always direct or obvious research and application areas can be found. One topic of interest in the graph is the vertical ***advertising***, which in turn leads to *ethical*. While ethics are not explicitly addressed in the descriptions of the focus actors in Table 2, this indicates it is a topic of interest in the application of technology to advertising.

Looking at the ***market***, co-occurring terms include *expert*, *domain*, *solution* and *customer*, indicating features considered in identifying markets.



Co-funded by the Horizon 2020 Framework Programme of the European Union

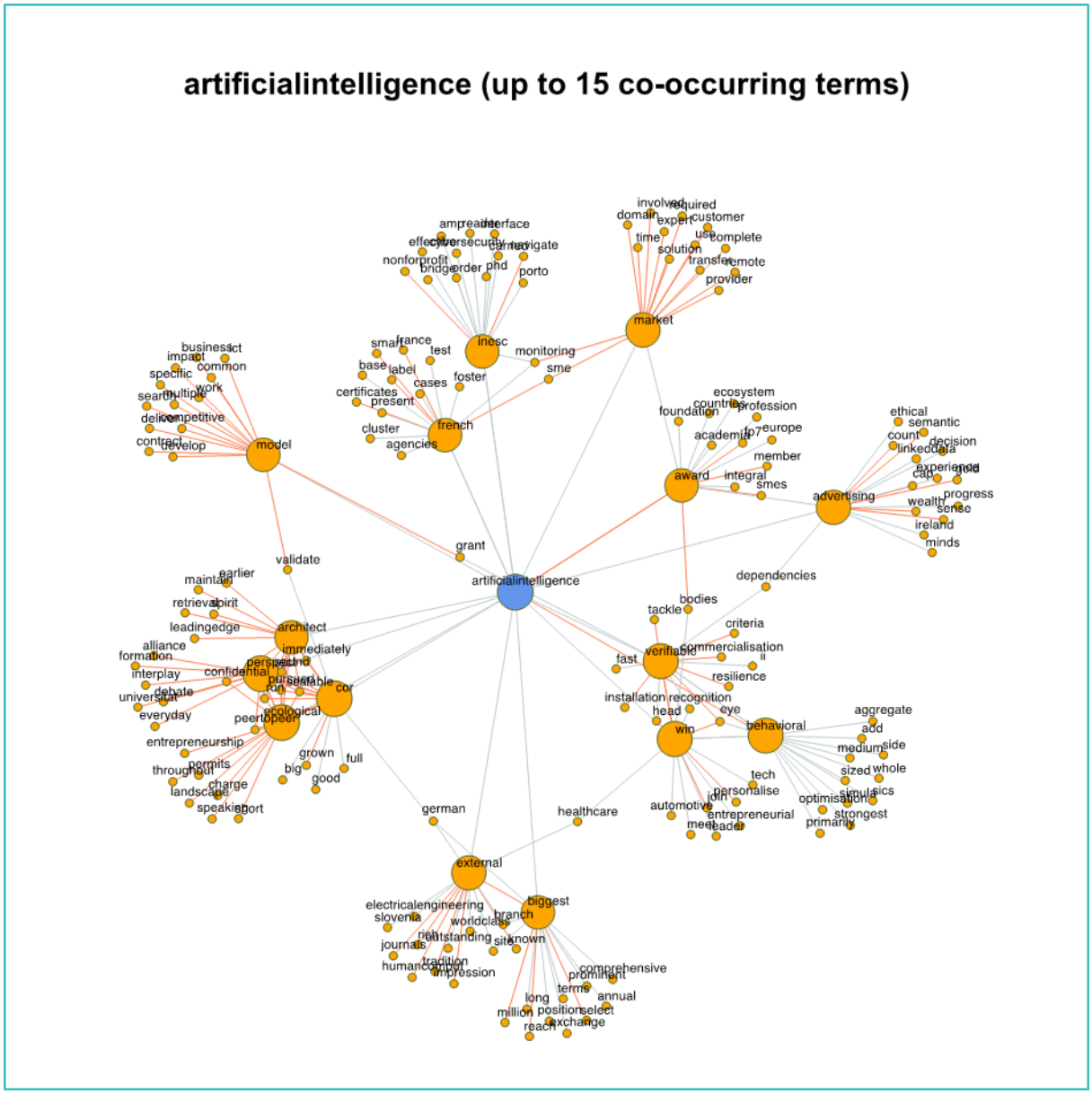


FIGURE 7: NETWORK ANALYSIS – ARTIFICIAL INTELLIGENCE

Figure 7 show the network analysis of AI and 15 most commonly associated terms. Significant links between topic pairs are coloured in orange.

## NGI Topic Internet of Things

A limitation in the examination of AI is a small sub-set within a relatively small dataset. Examining a more widely addressed topic broadens applicability of the results. We examine *IoT* - the *Internet of Things*, a topic that sees interest in application areas across home and work. Out of the 19 actors who use the term, three are universities. The remainder comprise 9 SMEs, a science park for *smart* technology and start-ups working on the technology.

The top 5 (by frequency of term mention) are all SMEs (see Table 3). Using a network such as that in Figure 7 we identify topics linked to IoT - including *cloud*, *big data* and *privacy*, with application to, among others, (the generation of) *certificates* and *mobile/mobility*.



Co-funded by the Horizon 2020
Framework Programme of the European Union

Table 3: Top 5 of 19 actors addressing IoT/Internet of Things

| | type | IoT | smart | cloud | big data | privacy | certificate | mobile(ity) |
|---|---|---|---|---|---|---|---|---|
| ControlThings Oy Ab | sme | 6 | 1 | 2 | 0 | 0 | 2 | 1 |
| Easy Global Market | sme | 5 | 2 | 0 | 0 | 0 | 2 | 0 |
| 3logic MK srl | sme | 2 | 0 | 0 | 0 | 0 | 0 | 2 |
| Silkroad 4.0 | sme | 3 | 0 | 0 | 0 | 0 | 0 | 1 |
| Modio Computing PC | sme | 2 | 1 | 2 | 1 | 2 | 0 | 0 |

To investigate what potential these actors may have for helping to identify markets in which to apply IoT-based solutions, we examine these 19 actors within the overall dataset. The dataset was split into 20 topics; Figure 8 shows the top 5 occurring/descriptive terms for each, and topic distribution for the 19 actors. The topic highlighted (red border), described by the terms ***develop***, ***solution***, ***software***, ***market*** and ***innovate***, sees, overall, the highest proportion across all 19 actors. This is in line with the types of organisations found in this subset. Actors 3, 8 and 10, followed by 7, 9 and 18, show very low probability of covering this topic. 7, 8 and 10 represent the three universities, and 3 is a research centre. 18 is an SME that focuses on smart buildings and equipment; the weighting here is unusually low. The remaining actors should serve as pointers to identifying application of IoT within target markets, and as test beds for solutions developed.

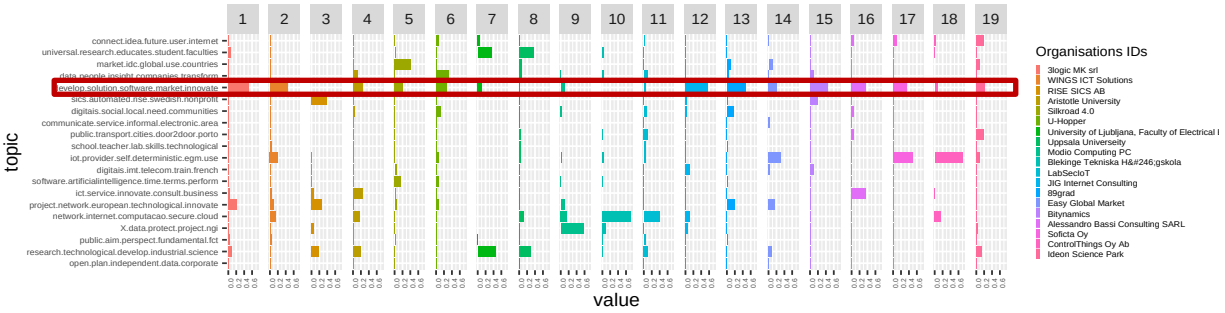


FIGURE 8: IOT ACTORS

Inspecting the top hit (see Figure 8), we confirm potential for this actor to play a part in enabling innovation pathways in *IoT*. In addition to development of smart technology to provide identities for objects within smart, connected networks, application to different targets is described. This actor therefore plays the part of a dual stakeholder - both a provider of expertise and an identifier of target markets.



Co-funded by the Horizon 2020 Framework Programme of the European Union


FIGURE 9: EXAMPLE OF NGI MAP

The key conclusion from this is that the map is a useful mechanism for locating collaborators, and since the map supports the recommended European innovation ecosystem involving many different participants of all kinds from across Europe, it is recommended that the map be sustained beyond the end of the HUB4NGI project.

#### 6.4.4.1 Statistics for NGI Community map

192 out of 194 actors provide descriptions, the other two are excluded from the stakeholder analysis. Of the 192 remaining, 99 mention at least one of the nine NGI key technology areas.

| Word counts - actor descriptions | |
|---|---|
| **Statistic** | **Value** |
| Mean | 87 |
| Median | 73 |
| Range | 11-387 |
| Word counts after pre-processing to remove stopwords | |
| **Statistic** | **Value** |
| Mean | 51 |
| Median | 44 |
| Range | 5-206 |



Co-funded by the Horizon 2020 Framework Programme of the European Union

| Actor Location | No. of countries | No. of Actors |
|---|---|---|
| EU | 22 | 176 |
| non-EU | 3 | 13 |
| non-Europe | 2 | 5 |
| Total | 27 | 194 |

| Actor Types | |
|---|---|
| Accelerator | 3 |
| Corporate | 5 |
| Civil Society Organisation | 3 |
| Co-working Space | 0 |
| Incubator | 3 |
| Influencer | 3 |
| Investor | 1 |
| NGI Contact Point | 24 |
| Non-Government Organisation | 11 |
| National Public Research Funding Org. | 1 |
| Public Organisation | 7 |
| Research Centre | 30 |
| Small Medium Enterprise | 44 |
| Start-up | 30 |
| University | 29 |



Co-funded by the Horizon 2020
Framework Programme of the European Union

# 7 REFERENCES


[1] 2017 INTERNET SOCIETY GLOBAL INTERNET REPORT: Paths to Our Digital Future. https://future.internetsociety.org/wp-content/uploads/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf

[2] Next Generation Internet 2025: A study prepared for the European Commission DG Communications Networks, Content & Technology, October 2018. https://nlnet.nl/NGI/reports/NGI-Study-ISBN-9789279864667.pdf

[3] Taylor, Steve, & Boniface, Michael. (2017, September 28). Next Generation Internet: The Emerging Research Challenges. Zenodo. http://doi.org/10.5281/zenodo.1284073

[4] Taylor, Steve, Pickering, Brian, Boniface, Michael, Anderson, Michael, Danks, David, Følstad, Asbjørn, Woollard, Fiona. (2018, July 2). Responsible AI – Key Themes, Concerns & Recommendations for European Research and Innovation (Version 1.0). Zenodo. http://doi.org/10.5281/zenodo.1303253

[5] Taylor, Steve, Pickering, Brian, Grace, Paul, Boniface, Michael, Bakir, Vian, boyd, danah, Zubiaga, Arkaitz. (2018, October 22). Opinion Forming in the Digital Age (Version 1.0). Zenodo. http://doi.org/10.5281/zenodo.1468576

[6] United Nations General Assembly, 1948. Universal Declaration of Human Rights. http://www.un.org/en/universal-declaration-human-rights/index.html

[7] Morganti, L, Ranaivoson, H, Mazzoli, E. Mediaroad – Vision Paper, The Future of Media Innovation, European Research Beyond 2020. http://www.mediaroad.eu/wp-content/uploads/2018/09/Vision-Paper_Future-of-Media-Innovation.pdf

[8] Will we still have a single global Internet in 2025? - The Ditchley Foundation https://www.ditchley.com/past-events/past-programme/2010-2019/2016/global-internet

[9] Richard Stevens, Giulia Carosella, Andrea Siviero & Steve Taylor HUB4NGI D1.3: NGI Impact Measures and Benchmarks

[10] Peter Van Daele, Aba-Sah Dadzie, & Steve Taylor HUB4NGI D3.2: Report for Prototyping and Validation

[11] Obar, J.A. and Oeldorf-Hirsch, A., 2018. The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. Information, Communication & Society, pp.1-20. https://doi.org/10.1080/1369118X.2018.1486870

[12] Adams, B., Clark, A. and Craven, J., 2018. It is Free and Always Will Be-Trading Personal Information and Privacy for the Convenience of Online Services. arXiv preprint arXiv:1804.08491.

[13] Reidenberg, J.R., Breaux, T., Cranor, L.F., French, B., Grannis, A., Graves, J.T., Liu, F., McDonald, A., Norton, T.B. and Ramanath, R., 2015. Disagreeable privacy policies: Mismatches between meaning and users' understanding. Berkeley Tech. LJ, 30, p.39.

[14] European Commission, “A European approach on Artificial Intelligence”, 25 April 2018. Available at: http://europa.eu/rapid/press-release_MEMO-18-3363_en.htm. Retrieved 2018-05-24.

[15] The European Group on Ethics in Science and New Technologies (EGE) http://ec.europa.eu/research/ege/index.cfm

[16] European Group on Ethics in Science and New Technologies (EGE), “EGE Statement on Artificial Intelligence, Robotics and ‘Autonomous’ Systems”, March 2018. Available at: http://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf. Retrieved 2018-05-22.

[17] European Economic and Social Committee (EESC), “Artificial intelligence – The consequences of artificial intelligence on the (digital) single market, production,




Co-funded by the Horizon 2020 Framework Programme of the European Union

consumption, employment and society", May 2017. Available at: https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/artificial-intelligence. Retrieved 2018-06-05.

[18] Horizon 2020 Work Programme 2018-2020 5.i. Information and Communication Technologies http://ec.europa.eu/research/participants/data/ref/h2020/wp/2018-2020/main/h2020-wp1820-leit-ict_en.pdf

[19] Horizon 2020 Work Programme 2018-2020 14. Secure societies - Protecting freedom and security of Europe and its citizens http://ec.europa.eu/research/participants/data/ref/h2020/wp/2018-2020/main/h2020-wp1820-security_en.pdf

[20] Horizon 2020 Work Programme 2018-2020 13. Europe in a changing world – Inclusive, innovative and reflective societies https://ec.europa.eu/research/participants/data/ref/h2020/wp/2018-2020/main/h2020-wp1820-societies_en.pdf

[21] Lehtiniemi, T., 2017. Personal Data Spaces: An Intervention in Surveillance Capitalism? Surveillance & Society, 15(5), pp.626-639.

[22] EU Commission: Annexes to the Proposal for a Decision of the European Parliament and of the Council on establishing the specific programme implementing Horizon Europe – the Framework Programme for Research and Innovation. Brussels, 7.6.2018 COM(2018) 436 final ANNEXES 1 to 3, https://eur-lex.europa.eu/resource.html?uri=cellar:7cc790e8-6a33-11e8-9483-01aa75ed71a1.0002.03/DOC_2&format=PDF

[23] The Economist Intelligence Unit: Next Generation Connectivity. October 2018, http://www.osborneclarke.com/insights/next-generation-connectivity-jeremy-kingsley-the-economist-intelligence-unit/.

[24] Huawei Technologies: Towards a New Internet for the Year 2030 and beyond – Future Networks. ITU-T, SG 13, 2018. https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201807/Documents/3_Richard%20Li.pdf.

[25] Networld2020: Smart Networks Vision – Strategic Research and Innovation Agenda. 2018, https://www.networld2020.eu/wp-content/uploads/2018/04/networld2020-5gia-sria-2018_draft-version-1.0-1.pdf.

[26] The data economy and the Next Generation Internet highlights from the digital assembly 2018 26 june 2018, Sofia (Bulgaria), Monique Calisti - July 2018

[27] IDC FutureScape: Worldwide Digital Transformation 2018 Predictions

[28] IDC Data Age 2025, November 2018

[29] Data-driven artificial intelligence for european economic competitiveness and societal progress, BDVA, November 2018 - http://www.bdva.eu/sites/default/files/AI-Position-Statement-BDVA-Final-12112018.pdf

[30] A study of big data evolution and research challenges, Deepak Gupta, Rinkle Rani, July 2018 - https://journals.sagepub.com/doi/abs/10.1177/0165551518789880



Co-funded by the Horizon 2020 Framework Programme of the European Union