|  |  |
| --- | --- |
|  | **Revision 1 toDocument EG-ITRs-2/5** |
| **8 January 2024** |
| **English only** |
|  |  |
| Contribution from Hill |
| USE OF AI IN INTERNATIONAL TELECOMMUNICATION SERVICES |
| **Purpose**To present information on the use of AI in international telecommunication services. **Action required**The Expert Group on the International Telecommunication Regulations is invited to **discuss** this document.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**Reference***Council* [*Resolution 1379*](https://www.itu.int/md/S23-CL-C-0121/en) *(Terms of Reference)*  [*EG-ITRs-1/2: Contribution from Hill: Overall considerations*](https://www.itu.int/md/S23-EGITRS1-C-0002/en) |

**Summary**

This contribution presents information on the current and future use of artificial intelligence (AI) on international telecommunication networks and submits that consideration should be given to adding provisions on such use of AI to the ITRs, in order to ensure the relevance of the ITRs which “consist of high-level guiding principles” in the current telecommunication/ICT environment.

**Background**

1. Pursuant to its Terms of Reference, the EG-ITRs may consider, among others, the relevance of the ITRs which “consist of high-level guiding principles" in the current telecommunication/ICT environment.

2. Issues regarding the use of AI in international telecommunication networks were first studied in ITU in 2018, in particular in a focus group (FG ML5G[[1]](#footnote-1)) of ITU-T Study Group 13 (SG13). On the basis of the output of that group, SG13 agreed several recommendations:

* “[Architectural framework for machine learning in future networks including IMT-2020](https://www.itu.int/rec/T-REC-Y.3172-201906-I/en)" (ITU-T Y.3172, June 2019)
* "[Machine learning in future networks including IMT-2020: use cases"](https://www.itu.int/rec/T-REC-Y.Sup55-201910-I) (Supplement 55 to Y.3170 Series, October 2019)
* "[Framework for evaluating intelligence levels​ of future networks including IMT-2020](https://www.itu.int/rec/T-REC-Y.3173-202002-I): (ITU-T Y.3173, February 2020)
* "[Framework for data handling to enable machine learning in future networks including IMT-2020](https://www.itu.int/rec/T-REC-Y.3174-202002-I):  ( ITU-T Y.3174, February 2020)
* [Machine learning marketplace integration in future networks including IMT-2020](https://www.itu.int/rec/T-REC-Y.3176-202009-P)” (ITU-T Y.3176, September 2020)​

3. We reproduce below the summary of Recommendation ITU-T Y.3172:

Recommendation ITU-T Y.3172 specifies an architectural framework for machine learning (ML) in future networks including IMT-2020. A set of architectural requirements and specific architectural components needed to satisfy these requirements are presented. These components include, but are not limited to, an ML pipeline as well as ML management and orchestration functionalities. The integration of such components into future networks including IMT-2020 and guidelines for applying this architectural framework in a variety of technology-specific underlying networks are also described.

4. Subsequently, it was agreed to continue the work in SG13, under Question 20/13 – Networks beyond IMT-2020 and machine learning: Requirements and architecture. That Question is currently active. We reproduce below the motivation of that Question:

The objective of this question is to study the requirements, architecture and use of technologies including artificial intelligence (AI)/machine learning (ML) to realize networks beyond IMT-2020, in order to address the anticipated needs of network and application services in the upcoming years.

5. At present, work in that Question includes work on draft Recommendation Y.IMT2020-AINDO-req-frame[[2]](#footnote-2). We reproduce below the draft summary of that Recommendation:

This Recommendation considers the comprehensive application of AI technologies in network design optimization with low cost, including network topology, link capacity, routing etc. It specifies functional requirements, framework and procedures for AI-based network design optimization in IMT-2020 networks and beyond.

6. As noted in 1.20 of our contribution [EG-ITRs-1/2](https://www.itu.int/md/S23-EGITRS1-C-0002/en), There appears to be an emerging consensus that, at a minimum:

1. AI systems should be transparent: it should be clear when something is AI-produced, and the training data and model architectures should be disclosed;
2. builders of AI systems should be made accountable for the outputs produced;
3. AI systems should not have full autonomous control of critical systems or infrastructure (which would include basic telecommunications infrastructure).

Indeed, a good summary[[3]](#footnote-3) of recent governmental actions around the world regarding AI use and its regulation identifies the above as among the themes that have emerged in those actions. The learned author of that summary concludes:

Some will compare the emerging AI policy movement to the emergence of policy machinery a century ago for automobiles or broadcasting, each of which spawned the creation of thousands of regulatory agencies and rules worldwide. Regardless, the global policy community will now need to make room for a new AI regulation function, whether or not it’s ready.

7. We note in this context that, in October 2023, the UN Secretary-General convened a High-Level Advisory Body on Artificial Intelligence[[4]](#footnote-4). The Body’s immediate tasks include building a global scientific consensus on risks and challenges, helping harness AI for the Sustainable Development Goals, and strengthening international cooperation on AI governance.

8. And that, on 30 October 2023, the G7 Summit adopted the Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI System[[5]](#footnote-5).

9. And that, also on 30 October 2023, the President of the United States of America issued an Executive Order directing actions that include[[6]](#footnote-6) “Promote the safe, responsible, and rights-affirming development and deployment of AI abroad to solve global challenges, such as advancing sustainable development and mitigating dangers to critical infrastructure.” Indeed section 11 (d) of the Executive Order[[7]](#footnote-7) states:

To address cross-border and global AI risks to critical infrastructure, the Secretary of Homeland Security, in coordination with the Secretary of State, and in consultation with the heads of other relevant agencies as the Secretary of Homeland Security deems appropriate, shall lead efforts with international allies and partners to enhance cooperation to prevent, respond to, and recover from potential critical infrastructure disruptions resulting from incorporation of AI into critical infrastructure systems or malicious use of AI.

10. Recent events regarding the Open AI organization reinforce the need for action. It appears that a dominant software company has, in effect, gained control of Open AI[[8]](#footnote-8). That company’s operating system is widely used, including in computers that provide critical infrastructure, including in the international telecommunication network. If AI is embedded in that operating system, without regulators or operating agencies being aware of the specifics of the embedded AI, then the AI could have unintended effects. For example, the AI could decide to cut off communications, on the grounds that it contributes to global warming, which must be avoided; or on the grounds that disinformation contributes to political unrest, which must be avoided.

11. A well respected and well known security expert has recently called for the regulation of AI, stating[[9]](#footnote-9): “We need AI transparency laws. When it is used. How it is trained. What biases and tendencies it has. We need laws regulating AI—and robotic—safety. When it is permitted to affect the world.”

12. The Council of Europe is developing a Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law public[[10]](#footnote-10). This indicates that a large number of developing countries believe that there is a need for treaty-level instruments to regulate certain aspects of AI.

13. Finally, and perhaps most importantly, the European Union has reached an agreement on harmonized binding rules on artificial intelligence (AI), the so-called artificial intelligence act[[11]](#footnote-11). According to this Regulation[[12]](#footnote-12), AI systems intended to be used as safety components in the management and operation of critical digital infrastructure are considered “high-risk AI systems” (see Annex III, 2(a) of the Regulation). Key provisions regarding high-risk AI systems can be summarized as follows:

1. high-risk AI systems are subject to certain requirements with respect to training data (Art. 10 of the Regulation),
2. high-risk AI systems must be transparent (Art. 13 of the Regulation),
3. high-risk AI systems must be subject to human oversight (Art. 14 of the Regulation), and
4. providers and users of high-risk AI systems must ensure compliance with the provisions of the Regulation (Arts. 16-21 and 29 of the Regulation).

14. If AI systems can affect the safety of the management or operation of the international telecommunication network (which is obviously a critical digital infrastructure), then they are subject to the provisions of the cited European Union Regulation.

15. In light of the above, we submit that consideration should be given to adding provisions on the use of AI in international telecommunication services, in order to ensure the relevance of the ITRs which “consist of high-level guiding principles” in the current telecommunication/ICT environment.

16. Specific suggestions regarding AI are given in no. 6 of Addendum 3 to our contribution [EG-ITRs-1/2](https://www.itu.int/md/S23-EGITRS1-C-0002/en), namely that consideration be given to adding provisions along the following lines to Article 3 of the ITRs:

b) Member States shall endeavour to ensure that AI systems used for the international telecommunication network are transparent: it should be clear when something is AI-produced, and the training data and model architectures should be disclosed.

c) Member States shall ensure that builders of AI systems used for the international telecommunication network are accountable for the outputs produced.

d) Member States shall ensure that AI systems do not have full autonomous control of critical systems or infrastructure used for the international telecommunication network (which would include basic telecommunications infrastructure).

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. <https://www.itu.int/en/ITU-T/focusgroups/ml5g/Pages/default.aspx> [↑](#footnote-ref-1)
2. <https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=18153> , accessed 27 October 2023. [↑](#footnote-ref-2)
3. https://thehill.com/opinion/technology/4389011-making-sense-of-2023s-tsunami-of-ai-policy-changes/ [↑](#footnote-ref-3)
4. <https://www.un.org/techenvoy/ai-advisory-body> [↑](#footnote-ref-4)
5. <https://www.mofa.go.jp/files/100573471.pdf> [↑](#footnote-ref-5)
6. FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence, available at:
<https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/> [↑](#footnote-ref-6)
7. <https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/> [↑](#footnote-ref-7)
8. <https://gizmodo.com/ai-safety-openai-sam-altman-ouster-back-microsoft-1851038439> [↑](#footnote-ref-8)
9. <https://www.belfercenter.org/publication/ai-and-trust> [↑](#footnote-ref-9)
10. <https://www.coe.int/en/web/artificial-intelligence/cai>
<https://www.coe.int/en/web/artificial-intelligence/home> [↑](#footnote-ref-10)
11. <https://www.consilium.europa.eu/en/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/> [↑](#footnote-ref-11)
12. <https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf> [↑](#footnote-ref-12)