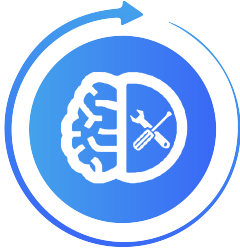


# Adversarial Robustness Toolbox Home

|                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  <h2 data-bbox="446 241 824 466">Adversarial Robustness Toolbox</h2> | <div data-bbox="876 216 1036 243">GRADUATE</div> <p data-bbox="1052 216 1445 331">Adversarial Robustness Toolbox (ART) provides tools that enable developers and researchers to evaluate, defend, certify and verify Machine Learning models and applications against the adversarial threats.</p> <p data-bbox="1052 352 1386 399">GitHub: <a href="https://github.com/Trusted-AI/adversarial-robustness-toolbox">https://github.com/Trusted-AI/adversarial-robustness-toolbox</a></p> |
|-------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Reference Information

- [Website](#)
- [Github](#)
- Primary Mail Lists
  - <https://lists.lfaidata.foundation/g/trusted-ai-360-announce>
  - <https://lists.lfaidata.foundation/g/trusted-ai-360-technical-discuss>
  - <https://lists.lfaidata.foundation/g/trusted-ai-360-tsc>

## Recent space activity

[Erin Thacker](#)  
[Adversarial Robustness Toolbox Home](#) updated Feb 17, 2022 [view change](#)

[Jacqueline Cardoso](#)  
[Adversarial Robustness Toolbox Home](#) updated Jan 20, 2021 [view change](#)



[Christina Harter](#)  
[Adversarial Robustness Toolbox Home](#) updated Dec 08, 2020 [view change](#)

[Jacqueline Cardoso](#)  
[Adversarial Robustness Toolkit - Community Meetings & Calendar](#) updated Aug 03, 2020 [view change](#)

## Space contributors

- [Erin Thacker](#) (819 days ago)
- [Jacqueline Cardoso](#) (1212 days ago)
- [Christina Harter](#) (1255 days ago)