

MPC GeoTools

GeoTools combined with Multi-Party Computation

Fabian Gruber

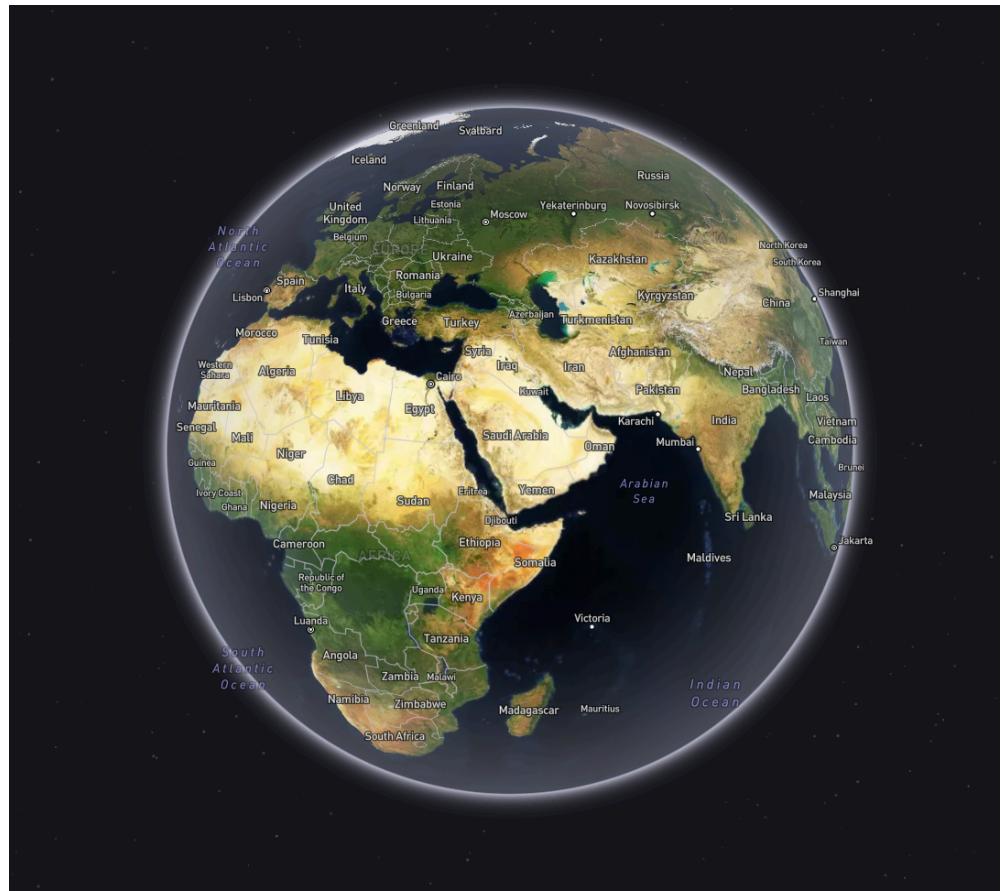
December 12, 2024

- Preserve privacy
- Secret computation with geo-spatial data
 - Distance between two parties
 - Bearing to other party
 - Check if inside area

- Sadly, the earth is not flat :(
- Computation would be much easier



- Earth is round (actually oblate spheroid, but who cares)
- Computation not as easy



Great-Circle Distance

- Distance between two points on sphere
- Haversine formula, chord length
- Points are (latitude φ , longitude λ)
- Secret-shared locations

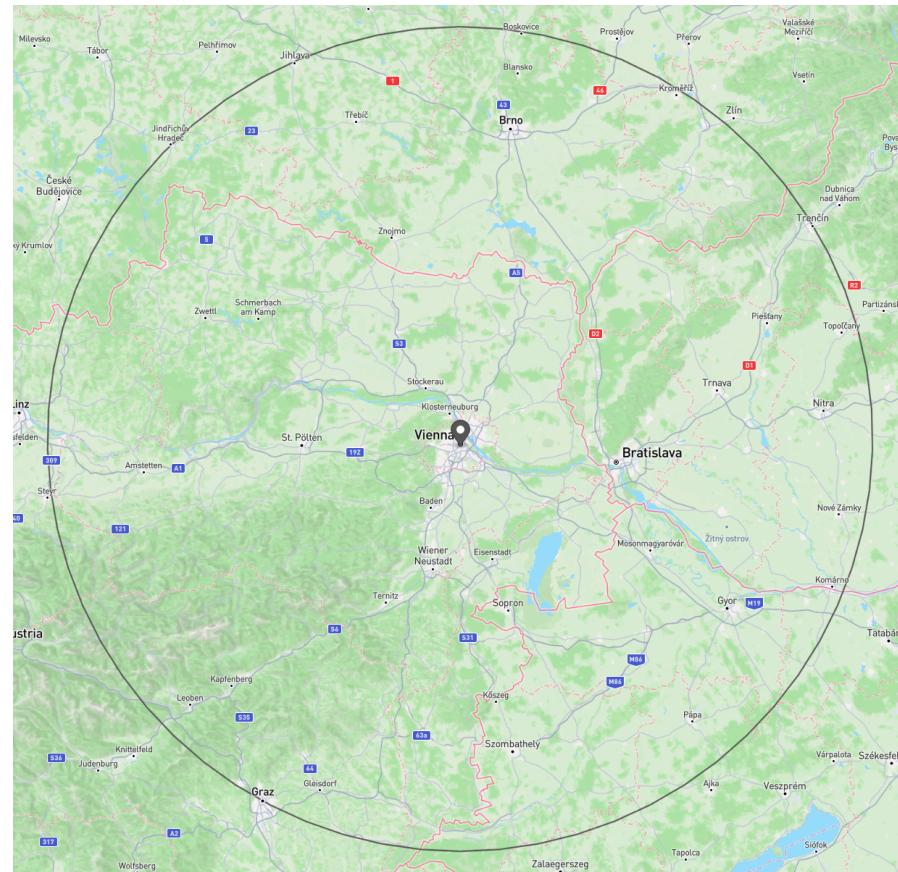
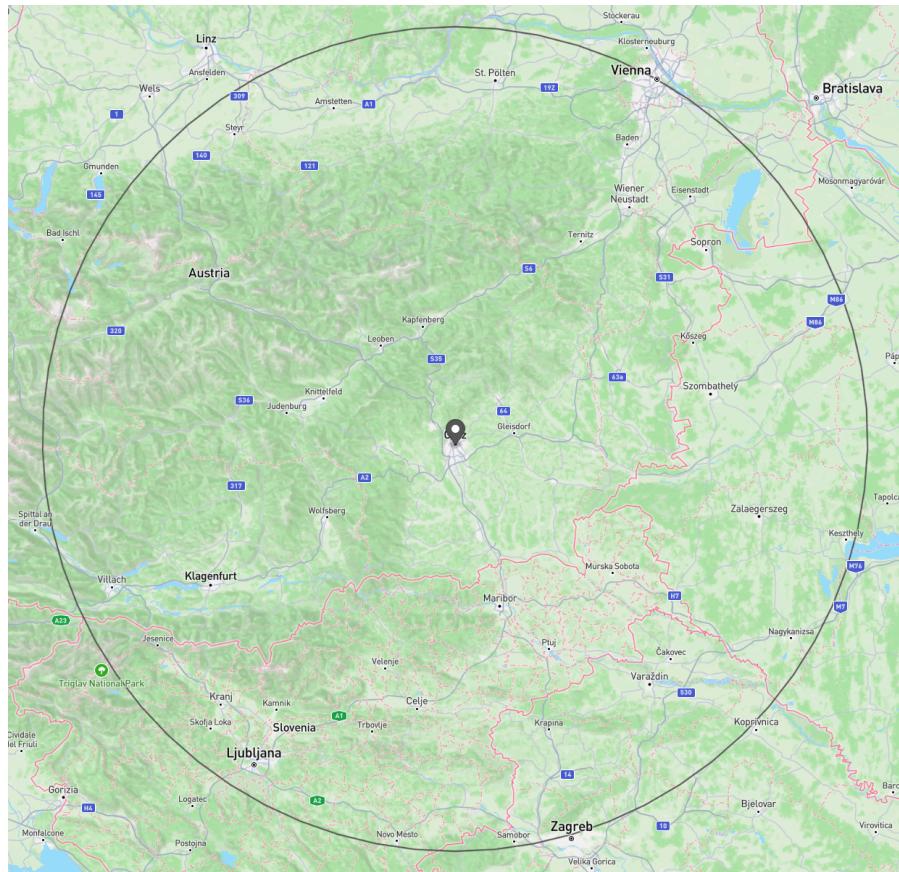
$$\Delta x = \cos \varphi_2 \cos \lambda_2 - \cos \varphi_1 \cos \lambda_1$$

$$\Delta y = \cos \varphi_2 \sin \lambda_2 - \cos \varphi_1 \sin \lambda_1$$

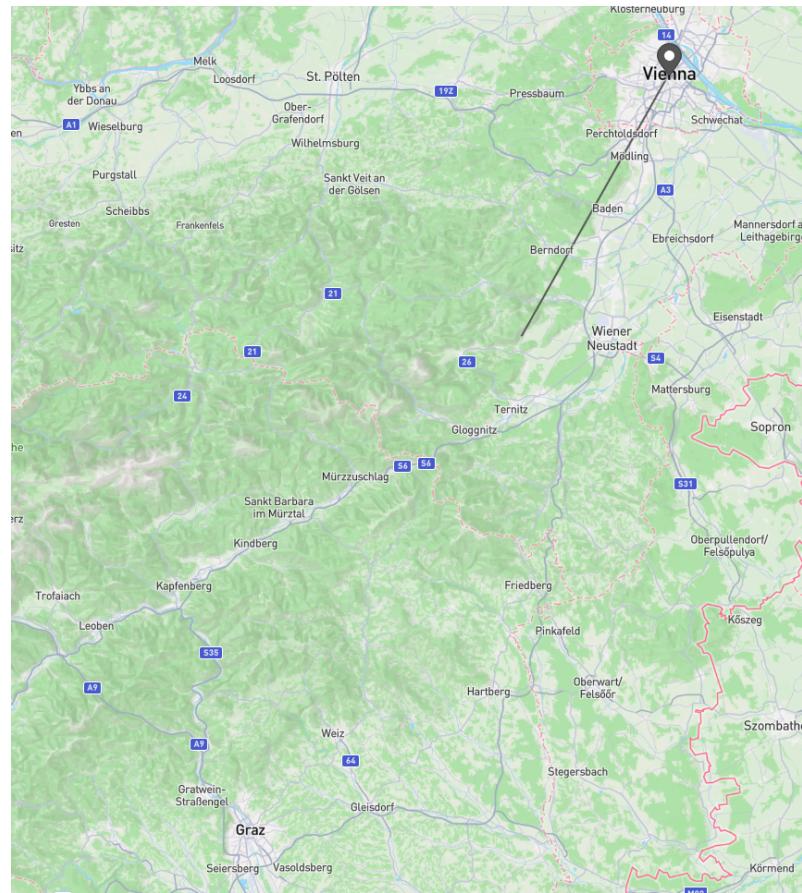
$$\Delta z = \sin \varphi_2 - \sin \varphi_1$$

$$\Delta\sigma_c = \sqrt{\Delta x^2 + \Delta y^2 + \Delta z^2}$$

Distance in MPC 144.55 km real 144.51 km

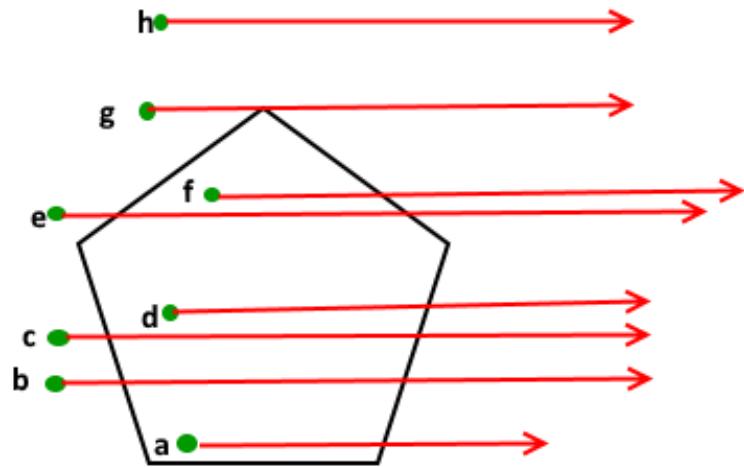


- Absolute bearing 209.42°
- Only initial bearing is revealed



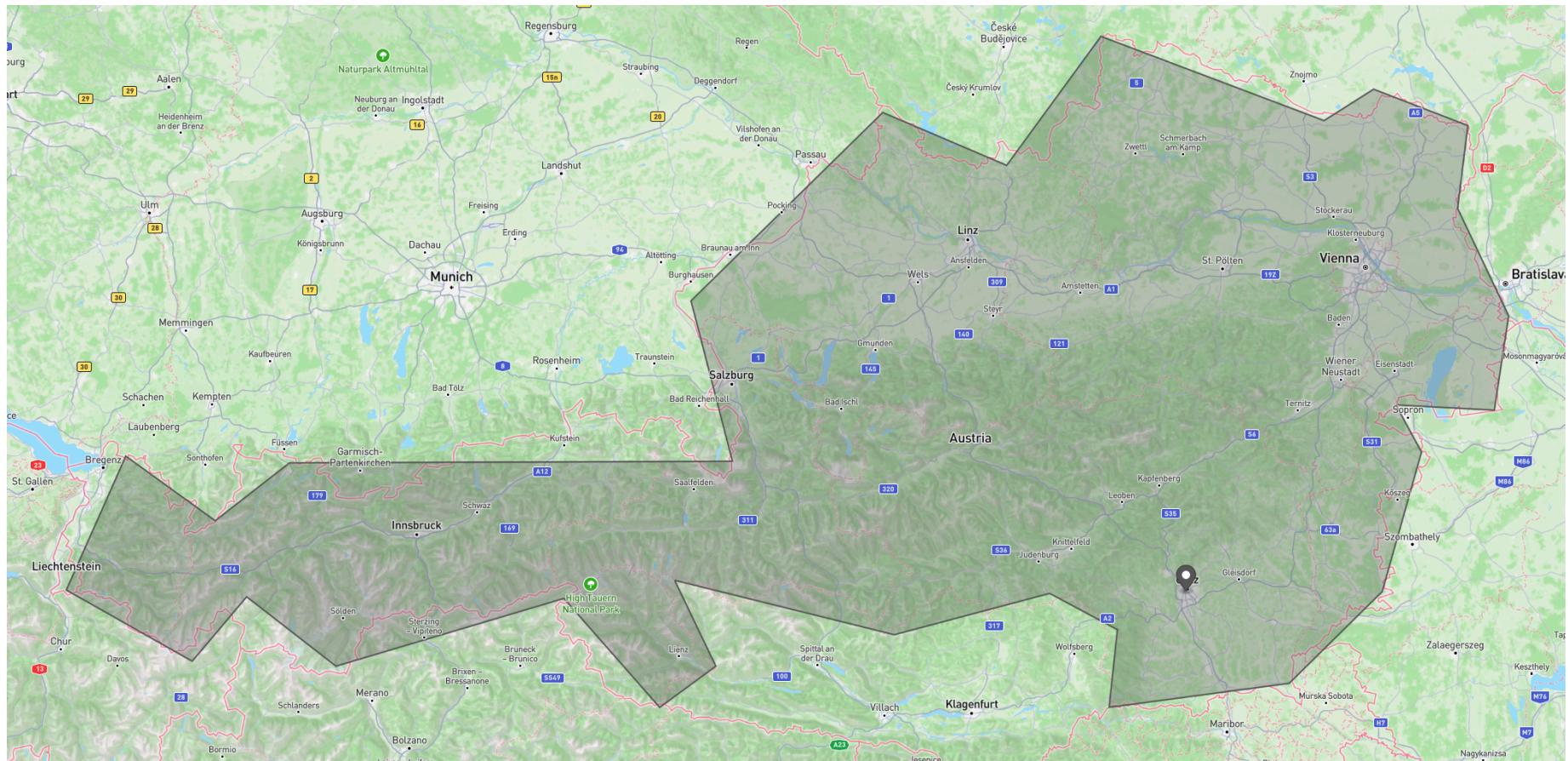
Point in Polygon

- Given the vertices of polygon on Mercator projection
- Return true if other party inside; else false
- Polygon can be public or secret



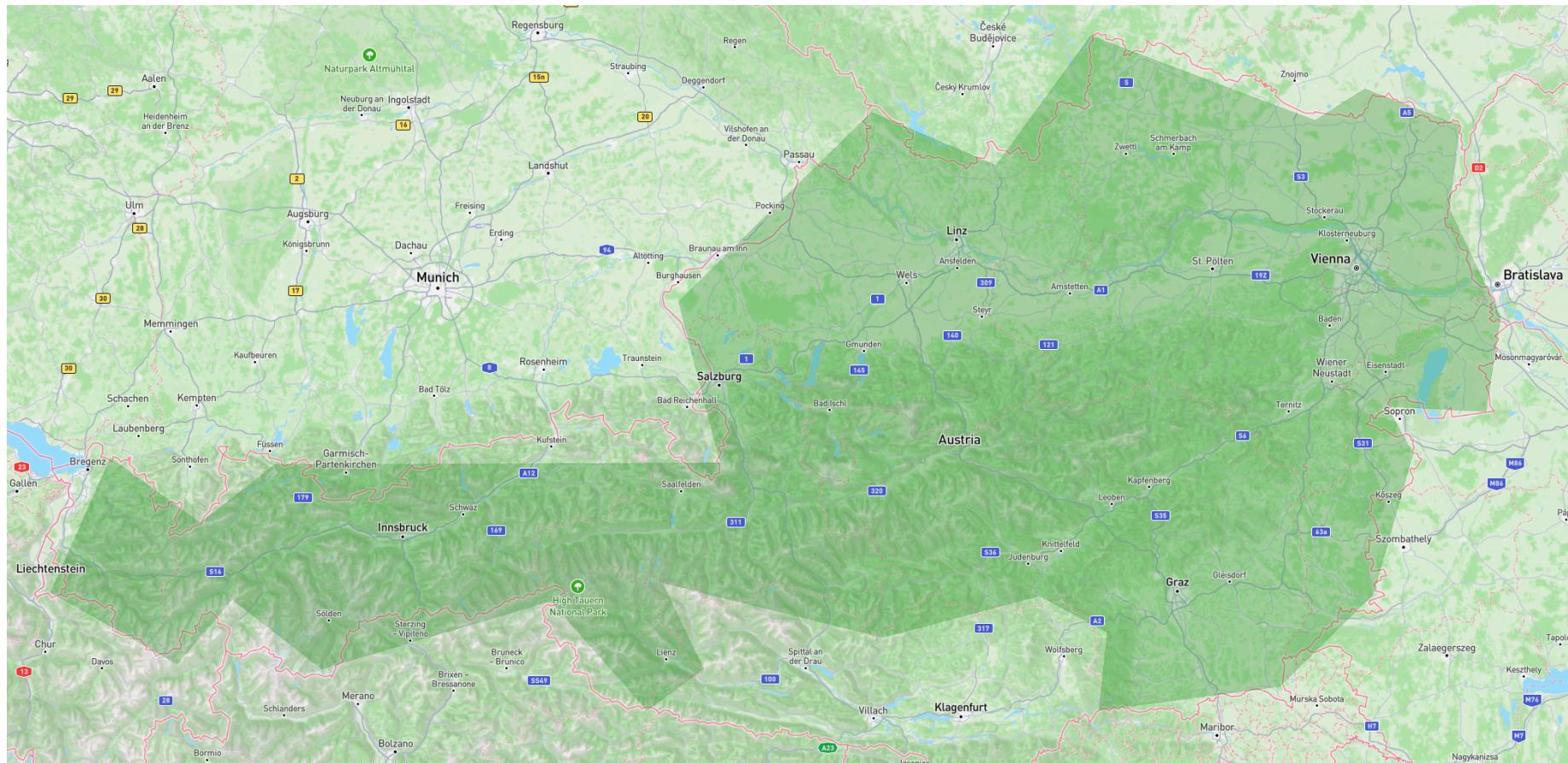
In Austria?

TACED



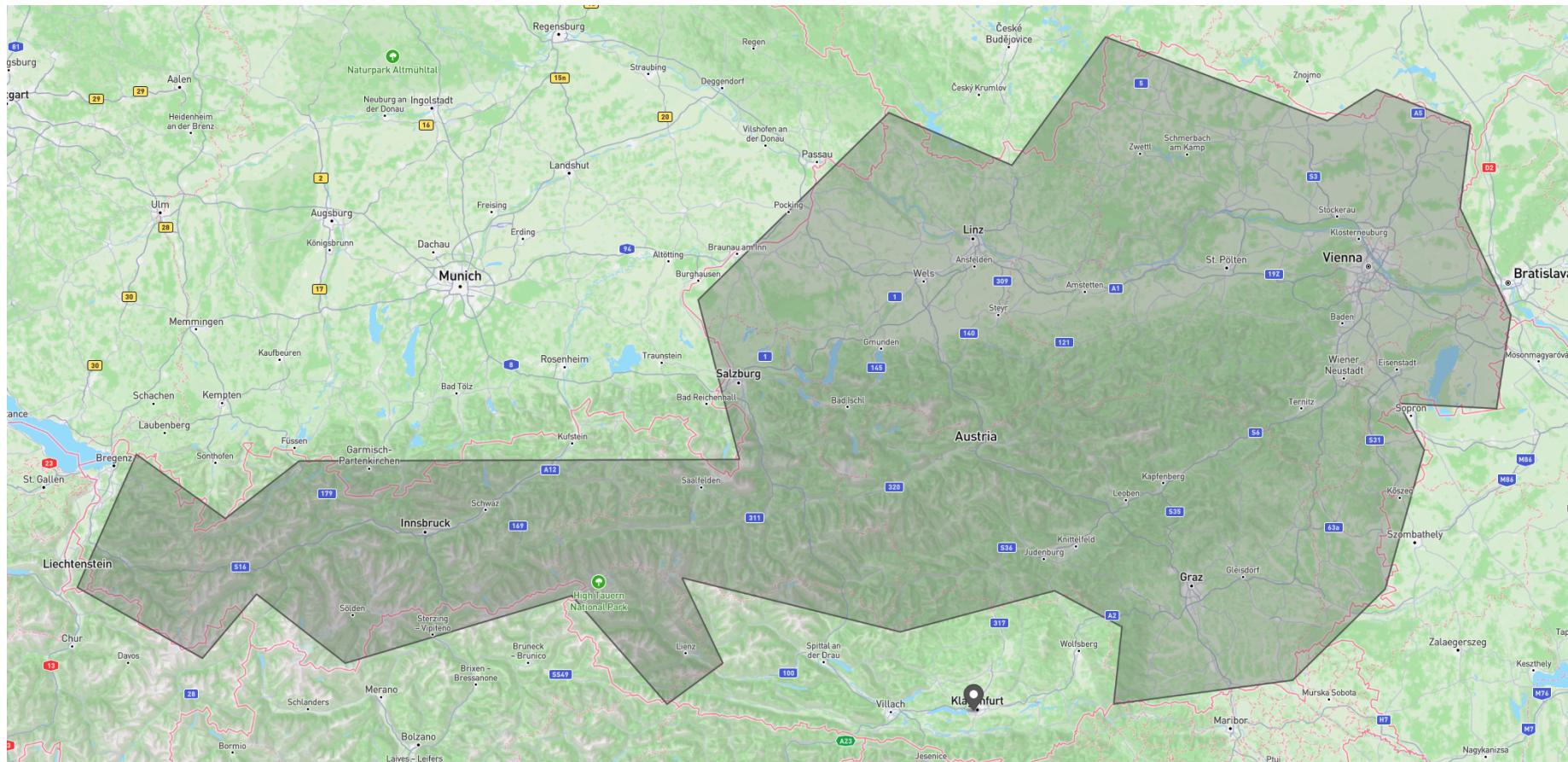
In Austria?

TACED



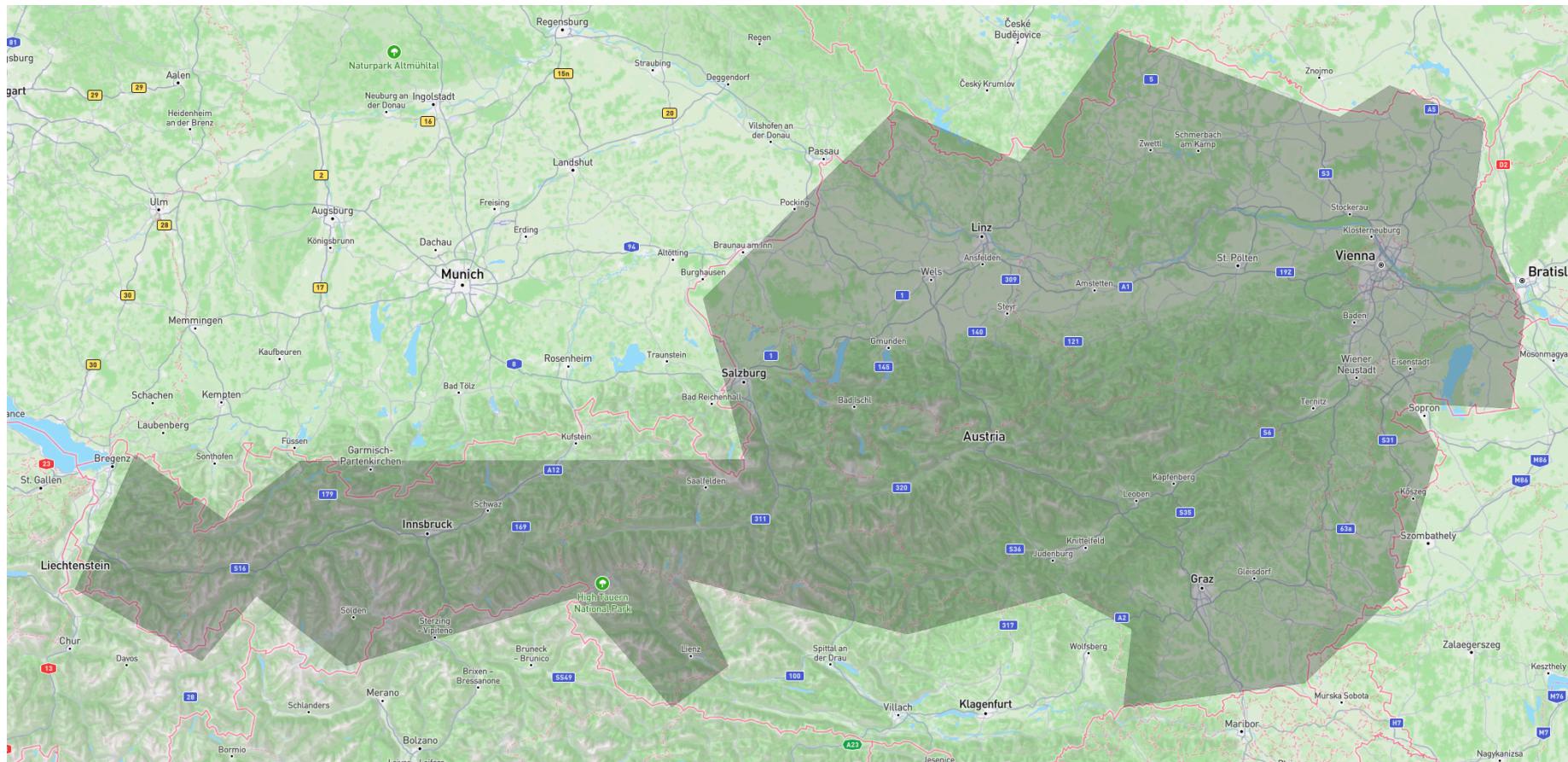
In Austria?

TACE



In Austria?

TAC3C



Thank you for your Attention!