

Motivation

- ▶ Detailed models of the power grid are **inaccessible for the security community**. However, power lines, substations and plants appear to be well documented by OpenStreetMap.
- ▶ **Is open geodata a reliable source of information?** Does open geodata provide worthwhile insights for adversaries?
- ▶ In this work, we **model** the Austrian power grid based on **OpenStreetMap Data**.

Processing the data in GIS

- ▶ **Import data** for each state where “power” is the key attribute and “line”, “minor line”, and “substation” are the values.
Clipping all vector layers, as the data are not linked to each other.
- ▶ **Generate geometric measurements** based on a selected CRS.
- ▶ **Calculate a buffer of 1km** for all substation objects to find out which lines might be connected to them.
- ▶ **Clipping all lines with the municipalities** where they run through.

Terms & Definition

Geographic Information System (GIS)

- ▶ Computer-aided system
- ▶ Model and process spatial data

Geodata

- ▶ Describe an object, either directly (by coordinates) or indirectly (e.g., by postal code), a landscape or by its position in space
- ▶ Can be linked to each other in order to create detailed queries and analyses

OpenStreetMap

- ▶ Built by a community of mappers that contribute and maintain open data about objects on the earth’s surface

QGIS

- ▶ Open source GIS for viewing, editing, and capturing spatial data
- ▶ OSM plugin allows the access to up-to-date OSM data, and simple export to an easy-to-use Shapefile or SQLite database

Maps & Tables

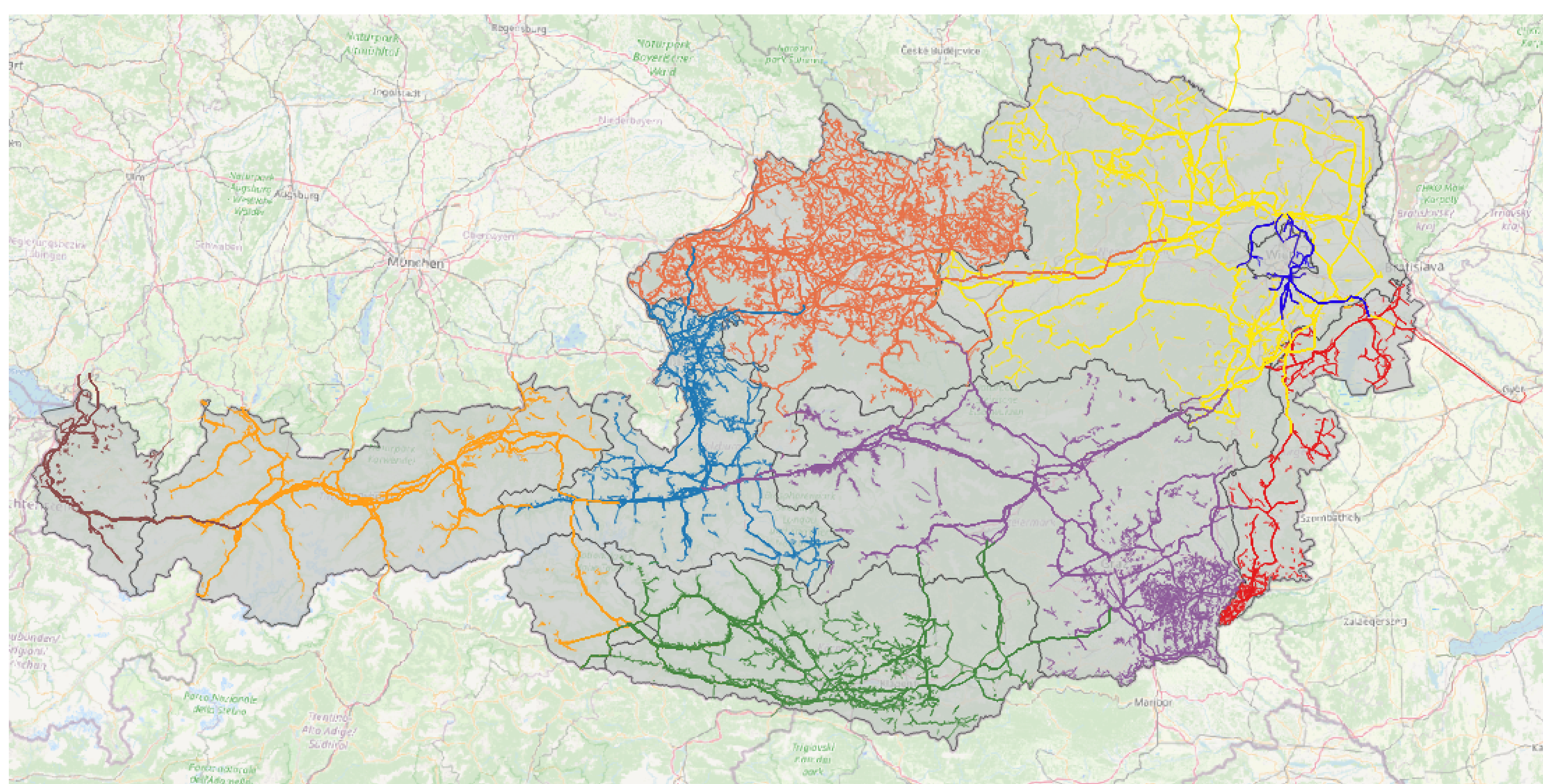


Figure 1: OpenStreetMap power lines Austria

ID	NAME	VOLTAGE	TYPE	STATUS	POWER	START	END	GEOMETRY	ATTRIBUTE
1	10kV	10	Line	Active	10	10.000000	10.000000	POINT(10 10)	10kV
2	20kV	20	Line	Active	20	20.000000	20.000000	POINT(20 20)	20kV
3	30kV	30	Line	Active	30	30.000000	30.000000	POINT(30 30)	30kV
4	40kV	40	Line	Active	40	40.000000	40.000000	POINT(40 40)	40kV
5	50kV	50	Line	Active	50	50.000000	50.000000	POINT(50 50)	50kV
6	60kV	60	Line	Active	60	60.000000	60.000000	POINT(60 60)	60kV
7	70kV	70	Line	Active	70	70.000000	70.000000	POINT(70 70)	70kV
8	80kV	80	Line	Active	80	80.000000	80.000000	POINT(80 80)	80kV
9	90kV	90	Line	Active	90	90.000000	90.000000	POINT(90 90)	90kV
10	100kV	100	Line	Active	100	100.000000	100.000000	POINT(100 100)	100kV

Figure 4: Attribute table QGIS – power lines

ID	NAME	VOLTAGE	TYPE	STATUS	POWER	START	END	GEOMETRY	ATTRIBUTE
1	10kV	10	Line	Active	10	10.000000	10.000000	POINT(10 10)	10kV
2	20kV	20	Line	Active	20	20.000000	20.000000	POINT(20 20)	20kV
3	30kV	30	Line	Active	30	30.000000	30.000000	POINT(30 30)	30kV
4	40kV	40	Line	Active	40	40.000000	40.000000	POINT(40 40)	40kV
5	50kV	50	Line	Active	50	50.000000	50.000000	POINT(50 50)	50kV
6	60kV	60	Line	Active	60	60.000000	60.000000	POINT(60 60)	60kV
7	70kV	70	Line	Active	70	70.000000	70.000000	POINT(70 70)	70kV
8	80kV	80	Line	Active	80	80.000000	80.000000	POINT(80 80)	80kV
9	90kV	90	Line	Active	90	90.000000	90.000000	POINT(90 90)	90kV
10	100kV	100	Line	Active	100	100.000000	100.000000	POINT(100 100)	100kV

Figure 5: Exported attribute table – including coordinates

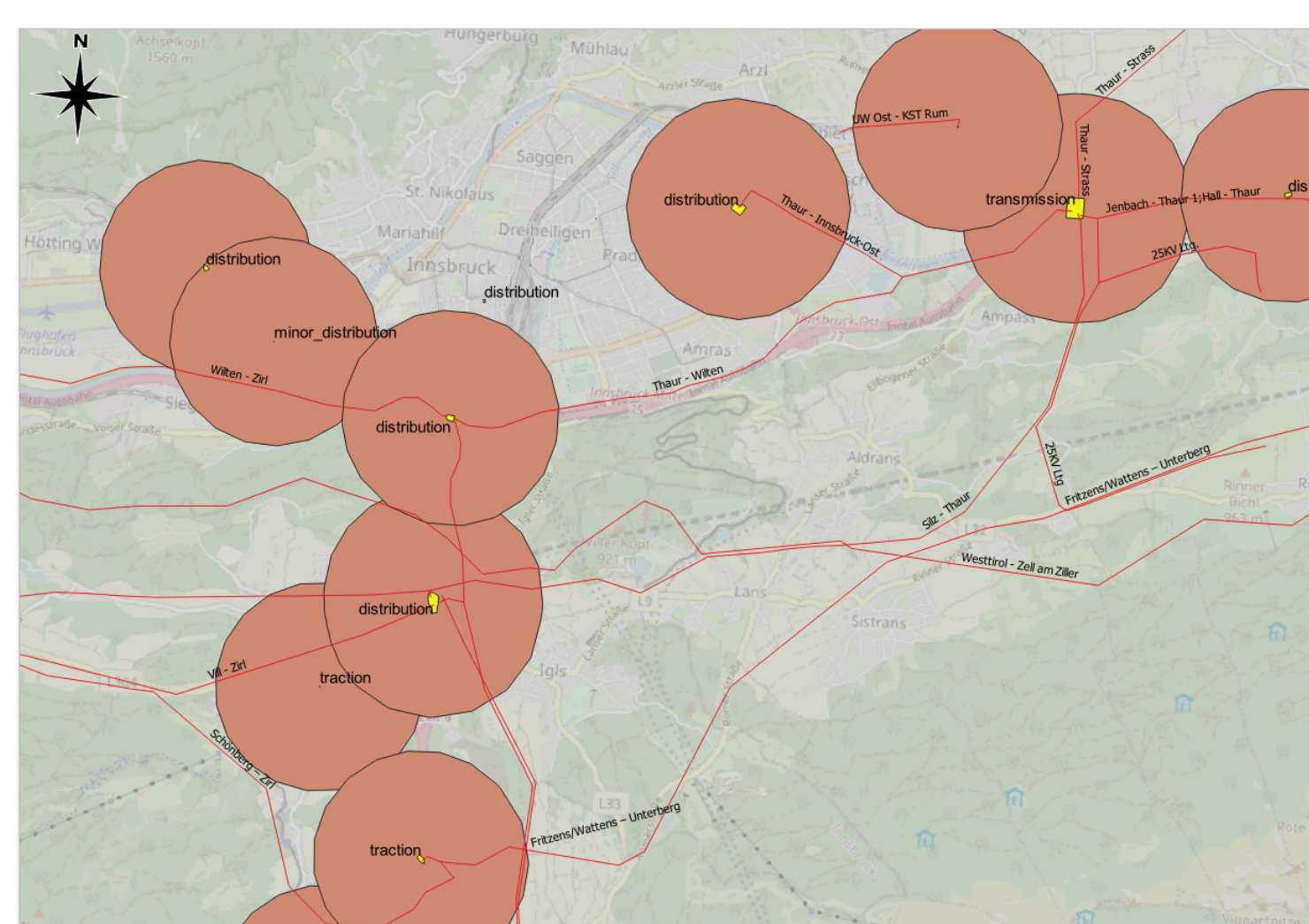


Figure 2: Buffer around substations

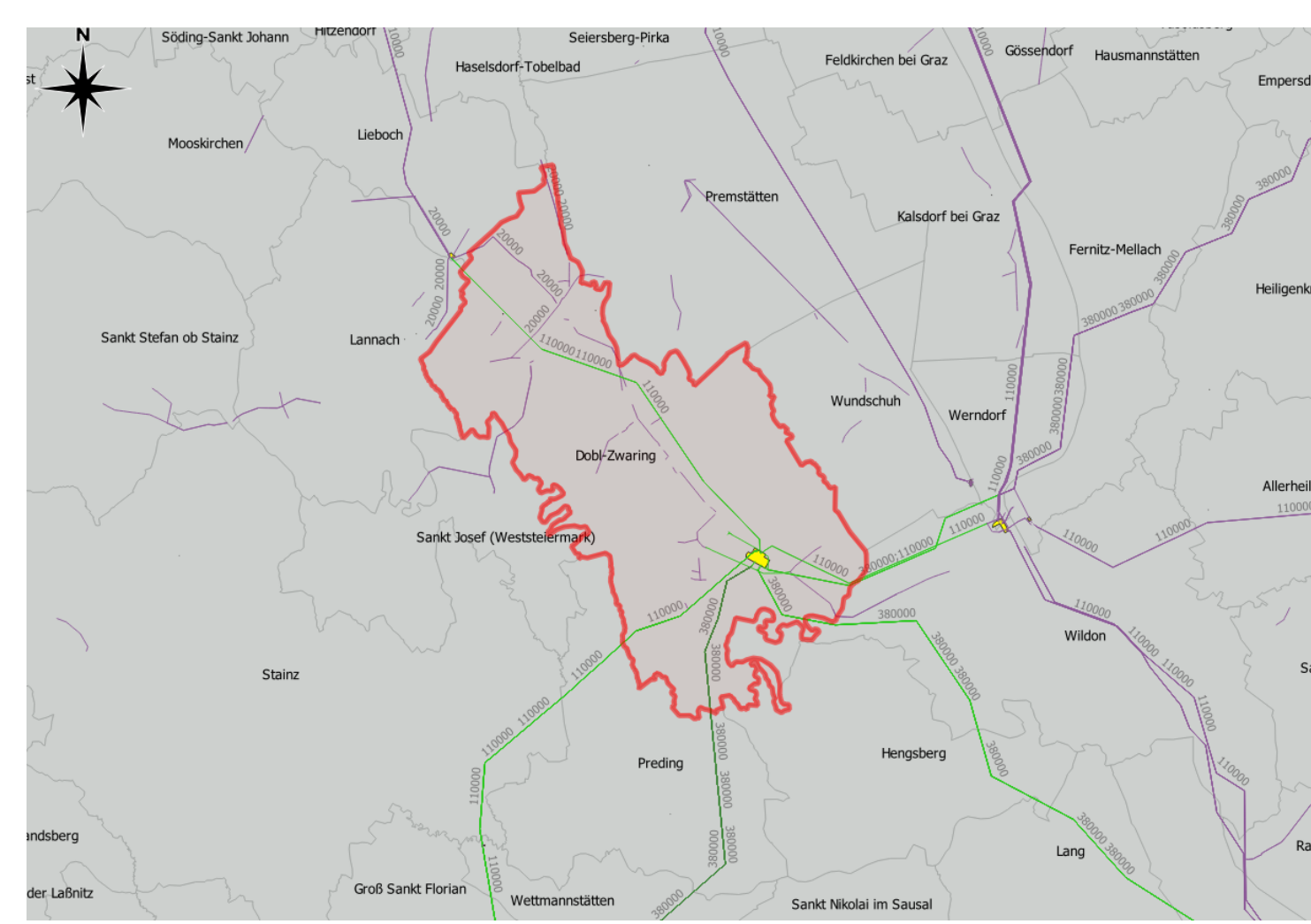


Figure 3: Power lines clipped with municipalities

ID	NAME	VOLTAGE	TYPE	STATUS	POWER	START	END	GEOMETRY	ATTRIBUTE
1	10kV	10	Line	Active	10	10.000000	10.000000	POINT(10 10)	10kV
2	20kV	20	Line	Active	20	20.000000	20.000000	POINT(20 20)	20kV
3	30kV	30	Line	Active	30	30.000000	30.000000	POINT(30 30)	30kV
4	40kV	40	Line	Active	40	40.000000	40.000000	POINT(40 40)	40kV
5	50kV	50	Line	Active	50	50.000000	50.000000	POINT(50 50)	50kV
6	60kV	60	Line	Active	60	60.000000	60.000000	POINT(60 60)	60kV
7	70kV	70	Line	Active	70	70.000000	70.000000	POINT(70 70)	70kV
8	80kV	80	Line	Active	80	80.000000	80.000000	POINT(80 80)	80kV
9	90kV	90	Line	Active	90	90.000000	90.000000	POINT(90 90)	90kV
10	100kV	100	Line	Active	100	100.000000	100.000000	POINT(100 100)	100kV

Figure 6: Attribute table QGIS – power lines clipped with municipalities

Conclusion & Future Work

- ▶ Based on the wide range of accessible geodata, we were **able to model the Austrian power grid**.
- ▶ Based on this model, we plan to **investigate attack strategies** using network analysis in the future.
- ▶ **Geodata provides worthwhile insights** for the security community and adversaries alike.
- ▶ **Security-by-obscurity cannot protect large-scale critical infrastructures** like the power grid.