SINA DÄUBENER

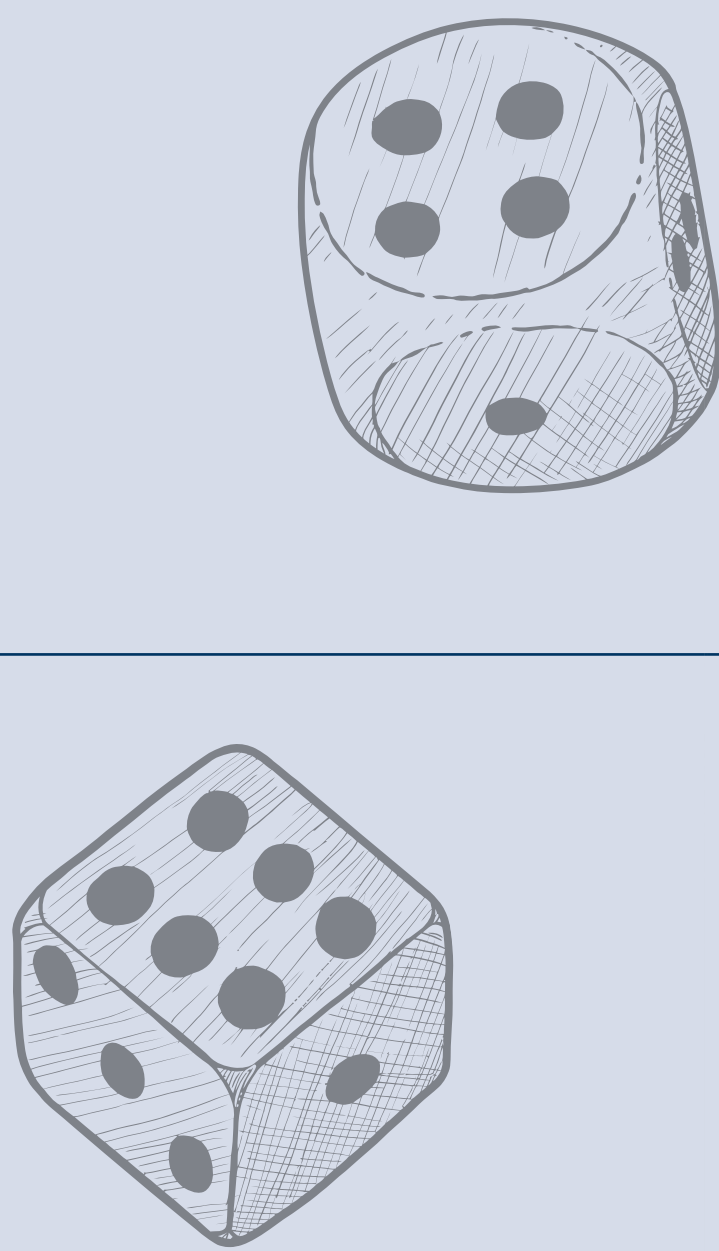UNCERTAINTY QUANTIFICATION
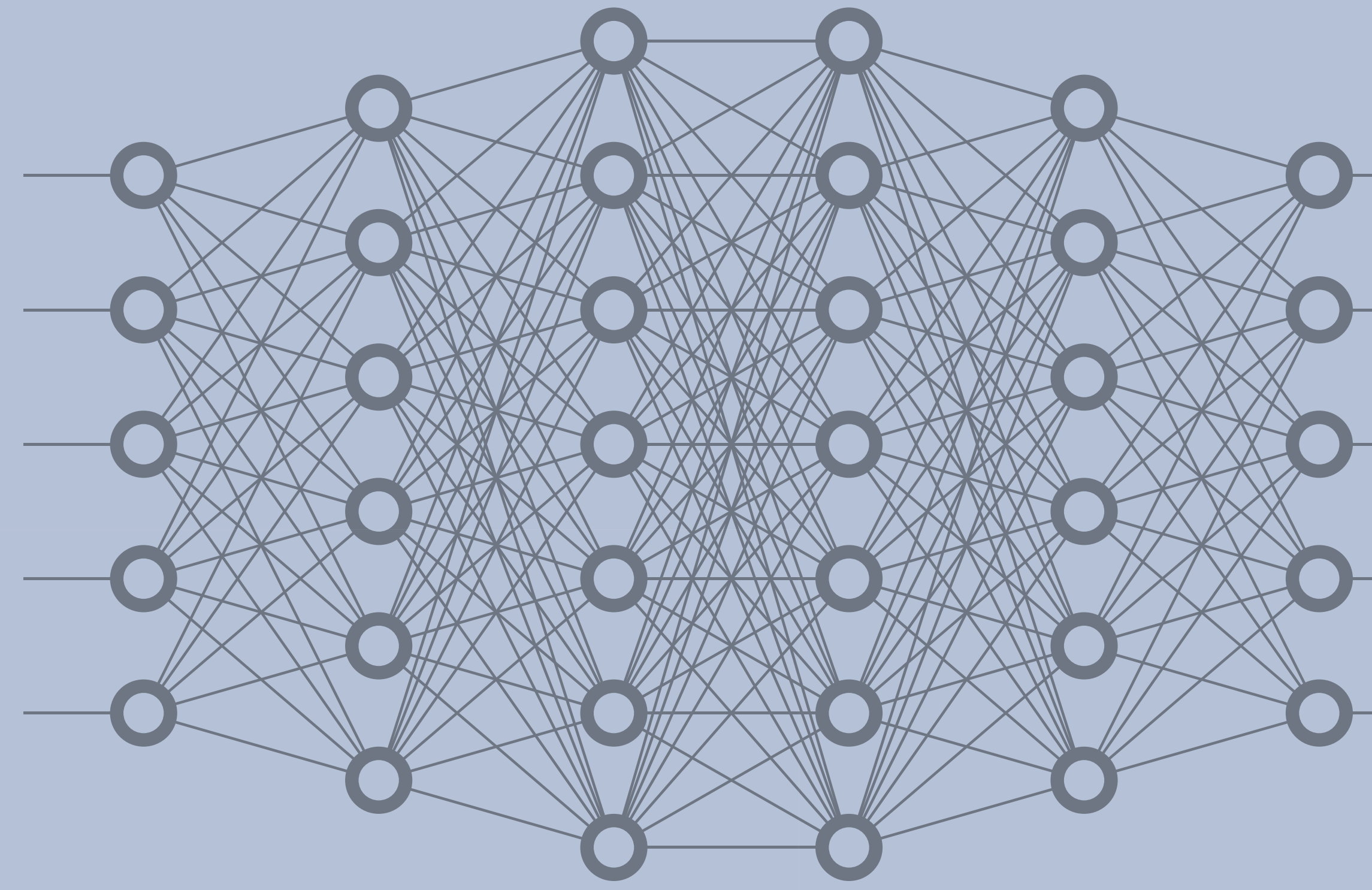
$$\int_\Theta p(y|x,\theta)q(\theta|\mathcal{D})d\theta$$

BAYESIAN NEURAL NETWORKS
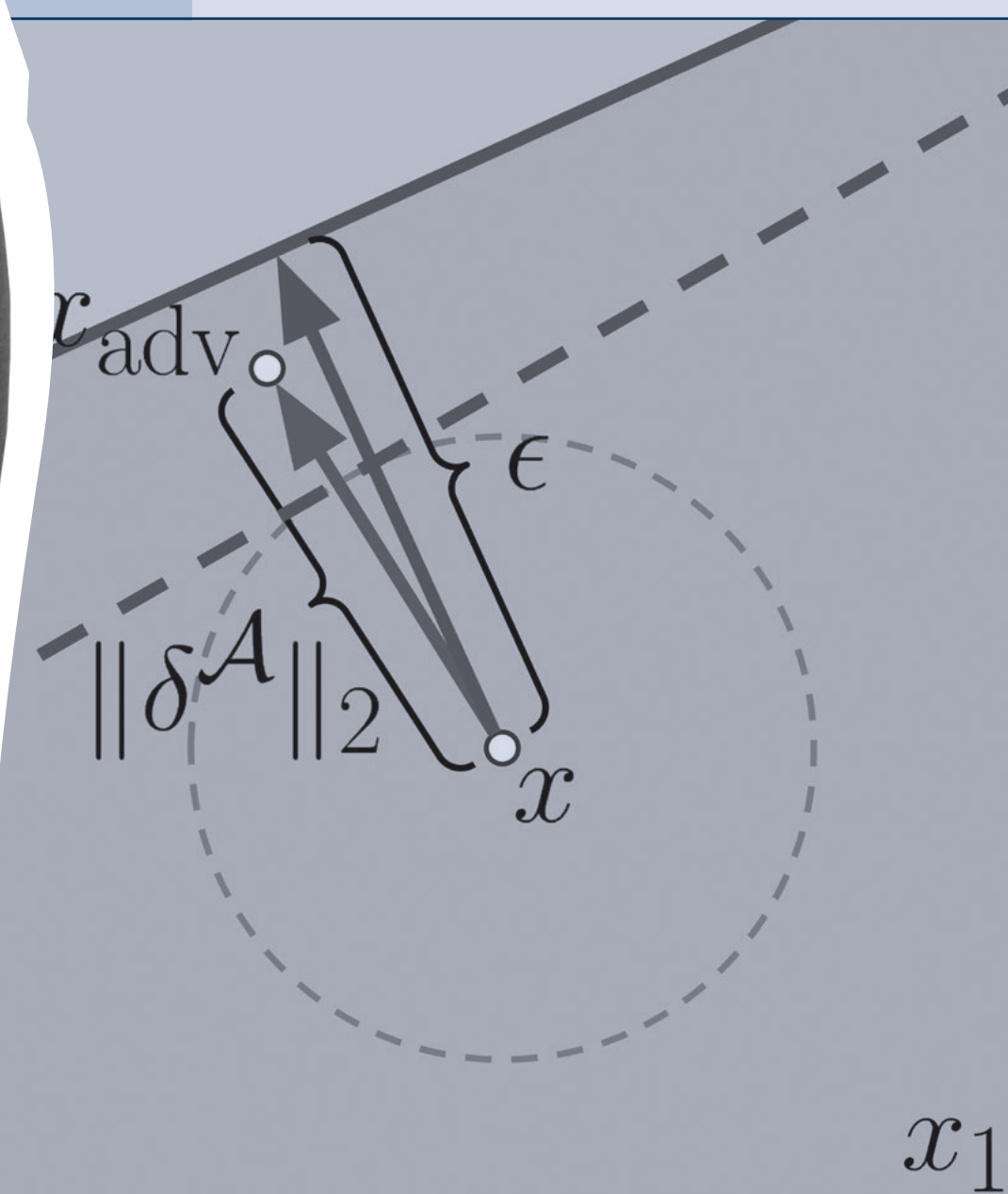
STOCHASTIC MODELS

ADVERSARIAL ROBUSTNESS

r_{adv}

ϵ

$\|\delta^{\mathcal{A}}\|_2$

x

x_1

WOMEN IN IT SECURITY

Sina Däubener is a PhD student at the Chair for Machine Learning at Ruhr-Universität Bochum (RUB), within the Cluster of Excellence CASA. Within her research, she investigates how stochastic neural networks can be used to detect and prevent adversarial attacks. In those, attackers add small perturbations to the input that lead to a malicious change in the network's prediction. She studied mathematics at the University of Münster, the Technical University of Valencia and the University of Düsseldorf, where she completed her master in 2017. Previous to her PhD, she worked as a data scientist on a European research project on improved energy and resource efficiency in the process industry.

CASA
Cyber Security in the Age of Large-Scale Adversaries

HGI HORST GÖRTZ INSTITUTE

RUB