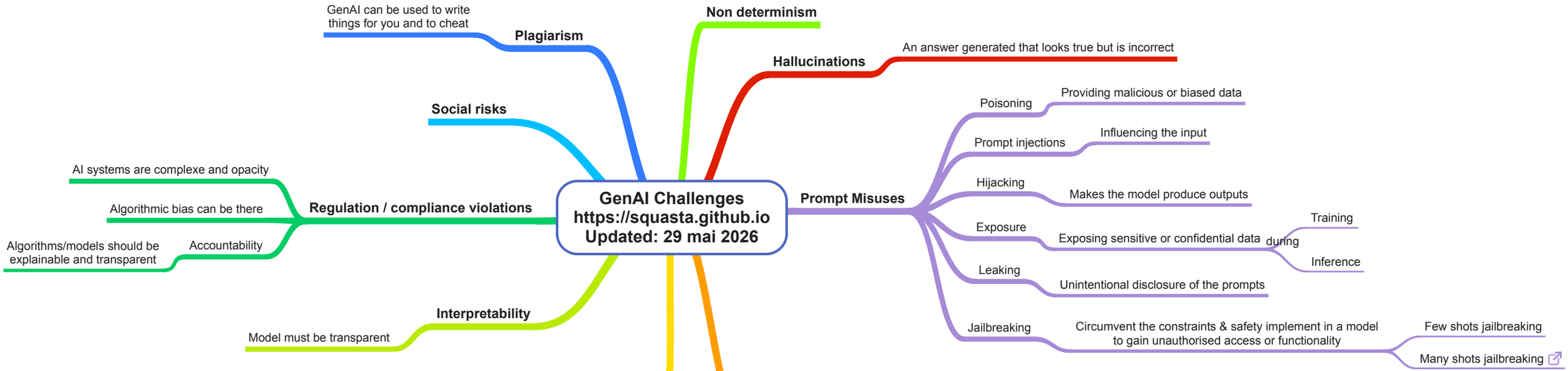
GenAI Challenges
https://squasta.github.io
Updated: 29 mai 2026
Plagiarism
GenAI can be used to write things for you and to cheat
Non determinism
Hallucinations
An answer generated that looks true but is incorrect
Social risks
Prompt Misuses
Poisoning
Providing malicious or biased data
Prompt injections
Influencing the input
Hijacking
Makes the model produce outputs
Exposure
Exposing sensitive or confidential data
during
Training
Inference
Leaking
Unintentional disclosure of the prompts
Jailbreaking
Circumvent the constraints & safety implement in a model to gain unauthorised access or functionality
Few shots jailbreaking
Many shots jailbreaking
Regulation / compliance violations
AI systems are complexe and opacity
Algorithmic bias can be there
Accountability
Algorithms/models should be explainable and transparent
Interpretability
Model must be transparent
Toxicity
Generate content offensive or inappropriate
How to prevent toxicity without censorship
Data security & Privacy risks
Data leak and exposure
Data poisoning