สำนักงานคณะกรรมการการรักษา
ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

The Future of Cybersecurity: AI, Quantum and Beyond

Soontorn Sirapaisan, PhD

Acting Head of the Research and Research Collaboration Section
Cybersecurity Research Center (CYBRE+)
National Cyber Security Agency (NCSA)
soontorn.s@ncsa.or.th

About Me

- Education
  - Bachelor's and Master's: Tsinghua University, China
  - PhD: The University of Manchester, UK
- Awards
  - Good Thesis Award by NRCT 2025
  - Recognition of Excellence 2023 by OpenGov Asia
  - ICT Innovation for eHealth & mHealth by MOPH
  - Good Innovation by NRCT
- Project
  - INTERVAC – International Vaccination Certificates
  - Guidelines for Post-Quantum Readiness
- Other Work Experiences
  - Consultant: Red Cross Society, DDC, DSI, …
  - Special Lecturer: SWU, PMK, SDU
  - Invited Speaker: domestic, international
- Contact
  - soontorn.s@ncsa.or.th , soontorn.sira@gmail.com
  - https://www.linkedin.com/in/soontorn-sirapaisan

What is Artificial Intelligence?

Image by Gerd Altmann from Pixabay

Prominent Types of AI in Use and Development

- It learns patterns and structures from vast amounts of training data (text, images, audio, code, etc.) and then generates novel outputs in various modalities.

Generative AI (GenAI)

- This is an emerging type of AI system designed to act autonomously to achieve specific goals with limited human supervision.

Agentic AI

- It allows computer systems to learn from and make decisions or predictions based on data, without being explicitly programmed for each task.

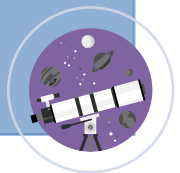
Machine Learning (ML)

- It enables machines to understand, interpret, generate, and respond to human language (both text and speech).

Natural Language Processing (NLP)

- It Allows AI systems to interpret and understand visual information from the world, such as images and videos.

Computer Vision

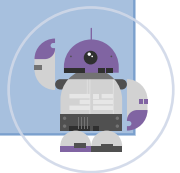


- AI programs designed to mimic the decision-making abilities of a human expert in a specific domain. They rely on a knowledge base and an inference engine.

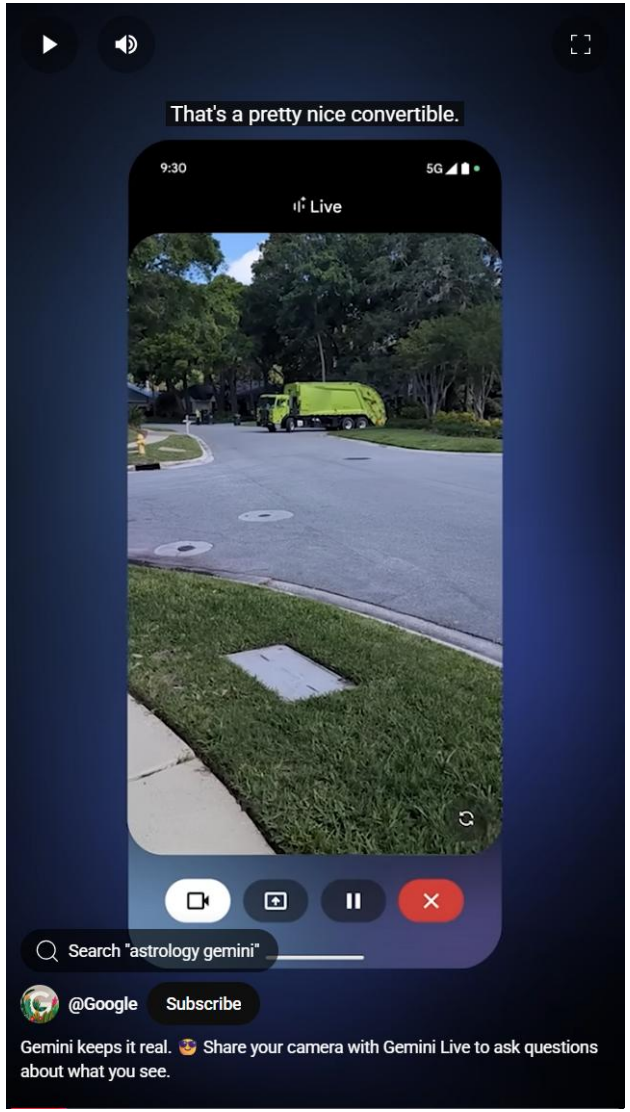
Expert Systems

- A field that involves designing, constructing, operating, and using robots. AI is often integrated into robots to give them intelligence and adaptability.

Robotics



You Can’t Trick Me!



https://www.youtube.com/shorts/aQKWQNbAH90

The Global Risks Report 2025

FIGURE C

Global risks ranked by severity over the short and long term

"Please estimate the likely impact (severity) of the following risks over a 2-year and 10-year period."

Source

World Economic Forum Global Risks Perception Survey 2024-2025.

World Economic Forum https://www.weforum.org/publications/global-risks-report-2025/

Deepfake CFO Tricks Finance Worker

https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html

Which are Real?

A

B

https://www.tidio.com/blog/ai-test/

This Person Does Not Exist

https://thispersondoesnotexist.com/

Which are Real?

https://www.tidio.com/blog/ai-test/

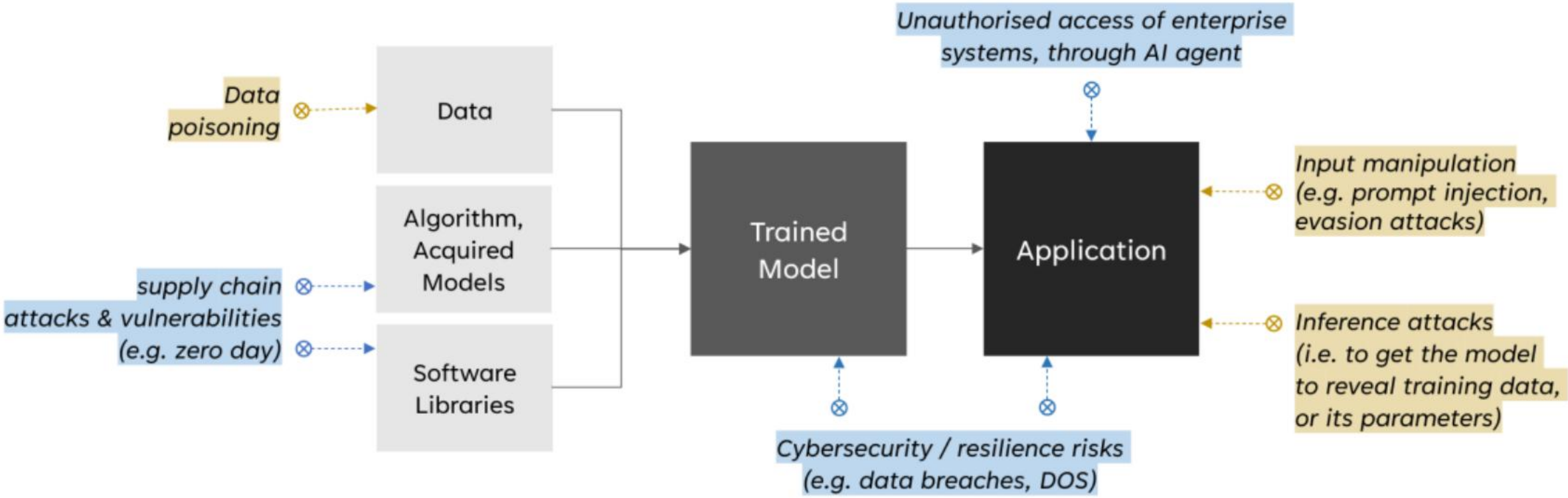
Use of AI in Enhancing Cybersecurity

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

NIST Cybersecurity Framework 2.0

Cyber Threats Against AI

Figure 1. Classical and AI-specific risks of AI systems– diagram adapted from OWASP[1]

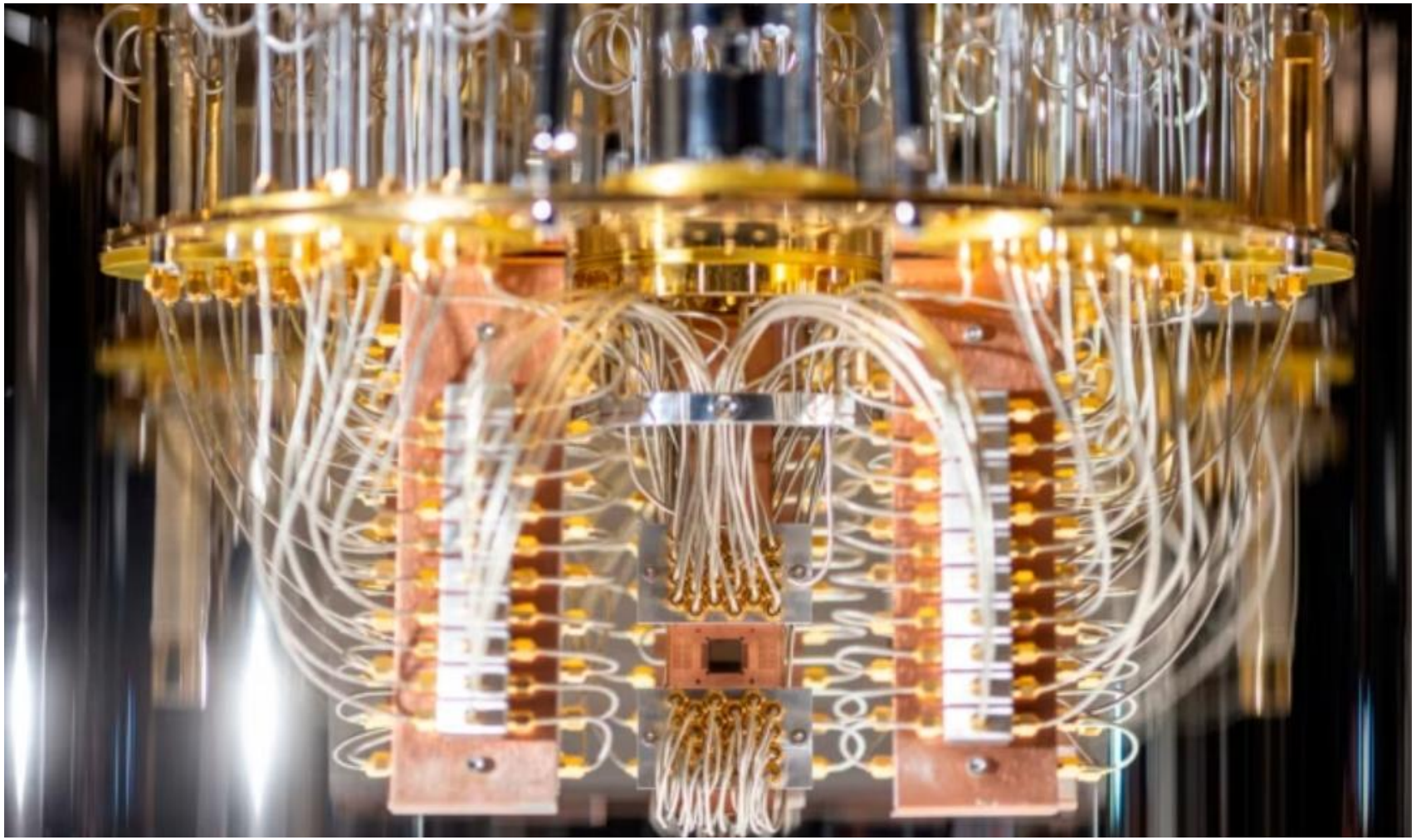


Cyber Security Agency (CSA) Singapore, "Guidelines on Securing AI Systems"

Concerns regarding AI Governance

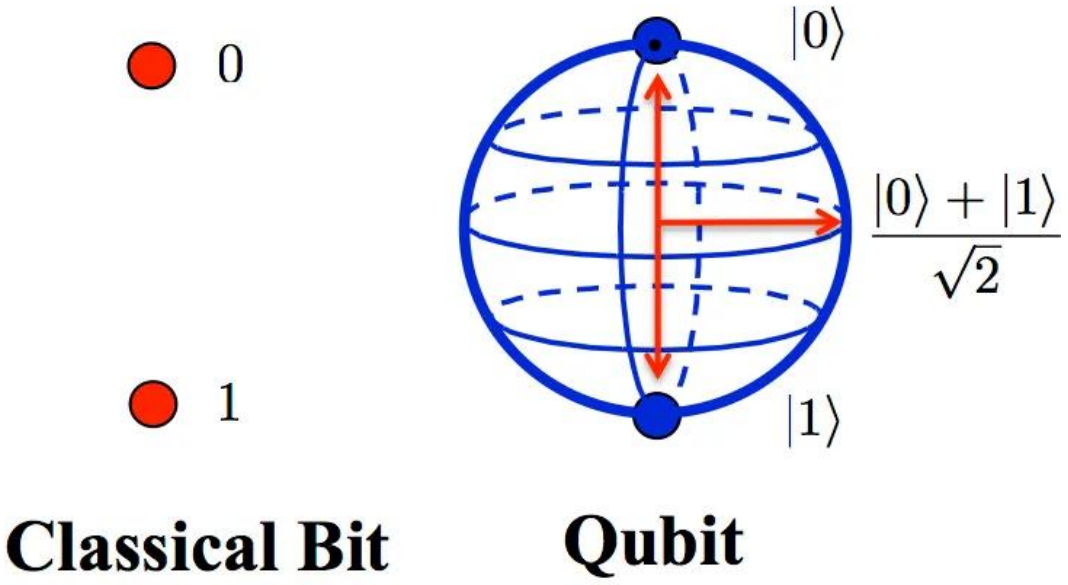
Ethical Considerations	Regulatory and Legal Challenges	Societal and Economic Impacts	Technical and Operational Challenges
• Bias and discrimination • Transparency and explainability • Accountability and responsibility • Human dignity and rights • Misuse of AI	• Keeping pace with technological advancement • Defining AI and its risk levels • Cross-jurisdictional issues • Implementing and enforcing regulations • Liability frameworks	• Job displacement and labor market transformation • Public trust and acceptance • Digital divide and inequality • Misinformation and manipulation • Environmental impact	• Data governance • Security • Monitoring and auditing • Standardization and interoperability

Quantum Computing

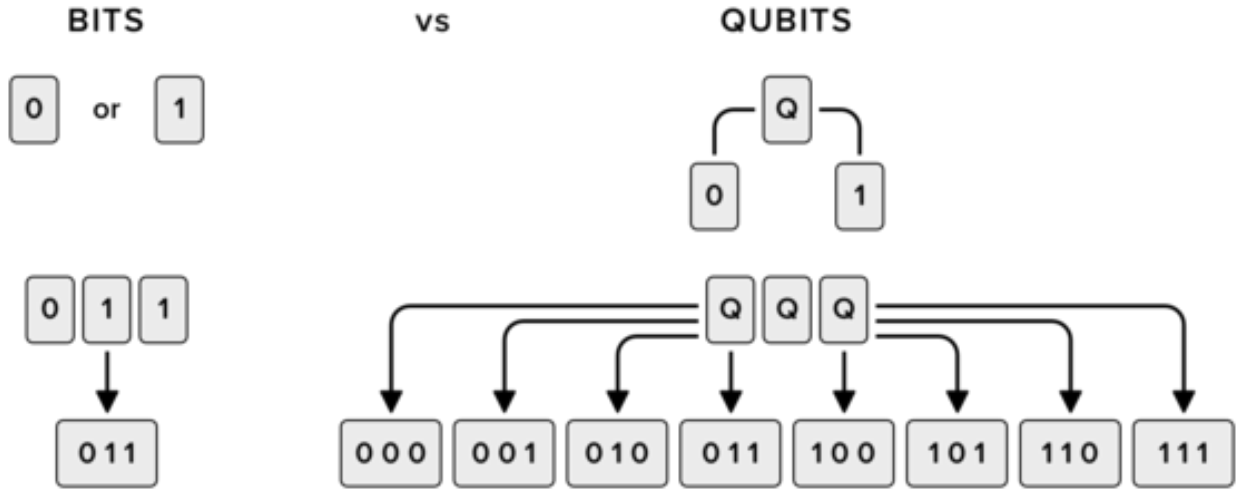


An early version of an IBM quantum computer on display at the company's London headquarters © Charlie Bibby/FT
https://www.ft.com/content/9ac38cf4-874e-4842-8be9-8fac2a3e898d

Classical Computer vs. Quantum Computer

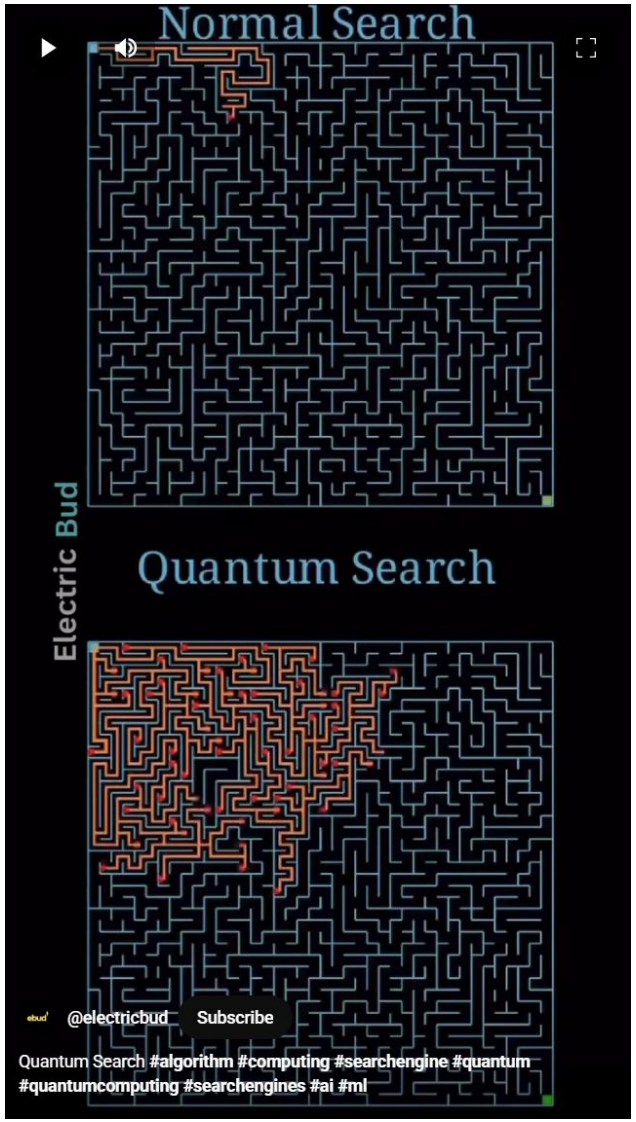


https://medium.com/@adubey40/classical-bit-vs-qubit-fa6c6c06e8f



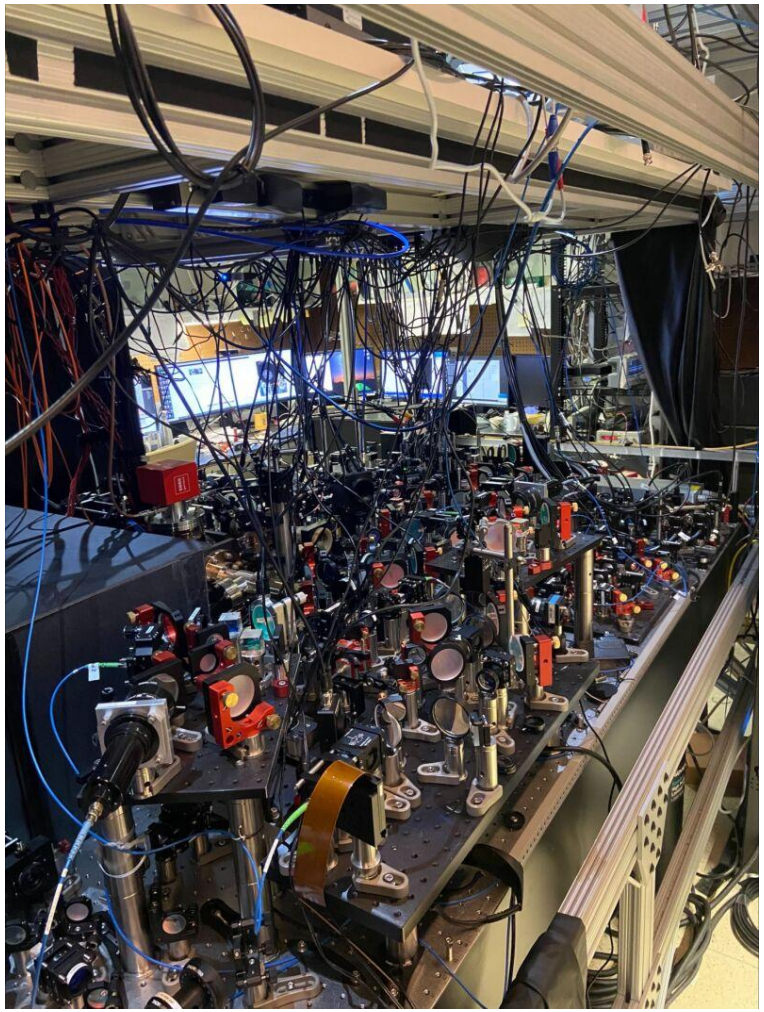
https://www.linkedin.com/pulse/classical-bit-vs-qubit-hafiz-muhammad-attaullah

Quantum Search



https://www.youtube.com/shorts/SCDQbju-D8o

An Example Quantum Computer QuEra



Harvard and QuEra get ready for error correction, run operations on 48 logical qubits.
https://arstechnica.com/science/2023/12/quantum-computer-performs-error-resistant-operations-with-logical-qubits/

Google Willow Chip

TECHNOLOGY › RESEARCH

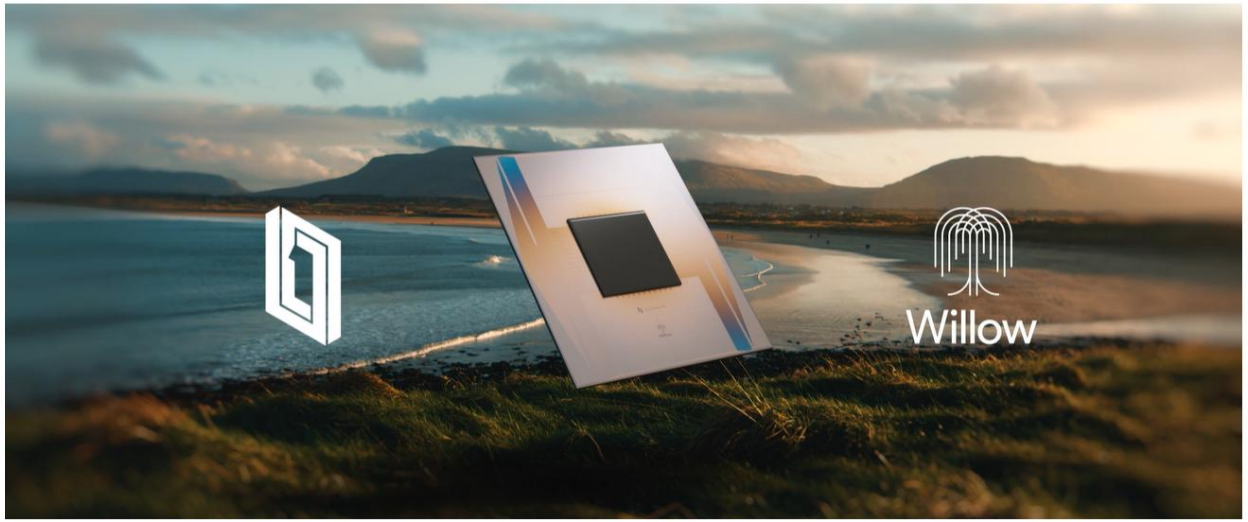
Meet Willow, our state-of-the-art quantum chip

Dec 09, 2024
6 min read

Our new chip demonstrates error correction and performance that paves the way to a useful, large-scale quantum computer

Hartmut Neven
Founder and Lead, Google Quantum AI

Read AI-generated summary Share



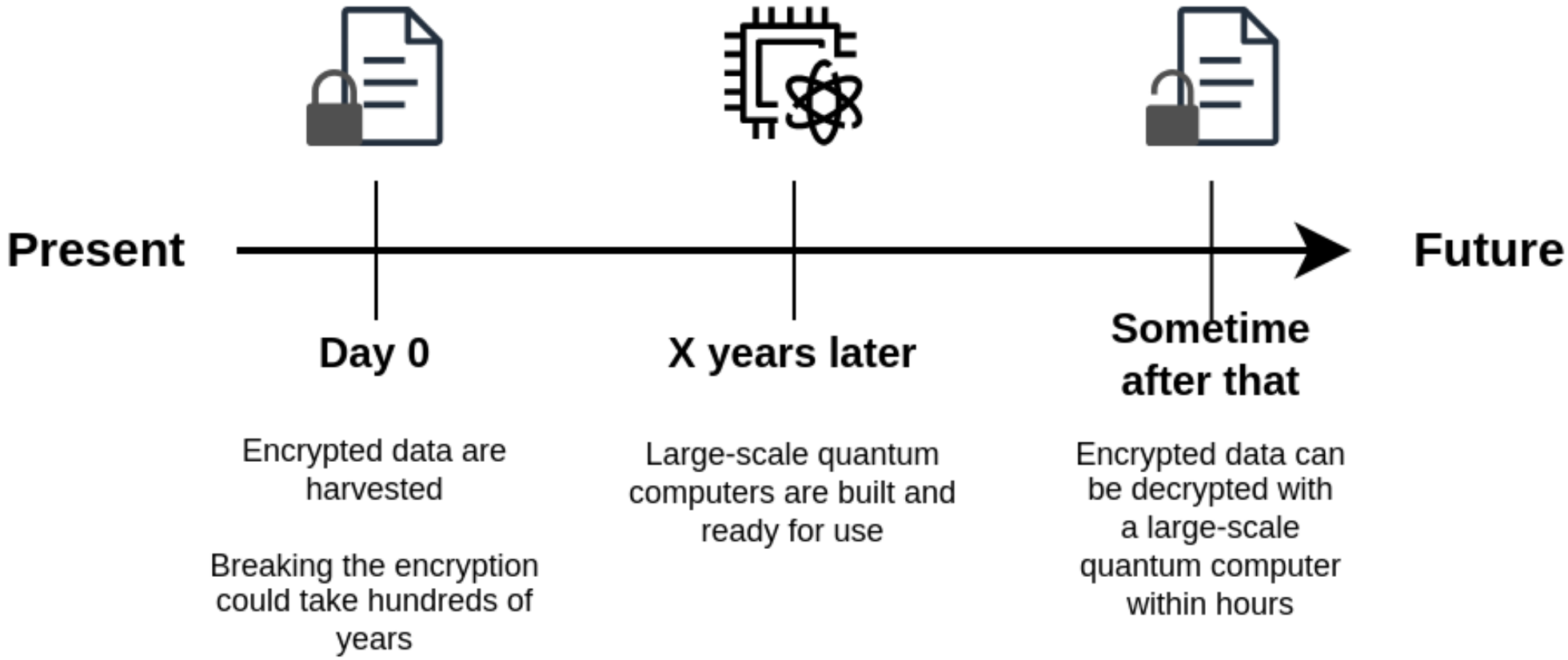
https://blog.google/technology/research/google-willow-quantum-chip/

Benefits of Quantum Computing

- Complex problems are problems with lots of variables interacting in complicated ways, for example,
  - Modeling the behavior of individual atoms in a molecule is a complex problem
  - Speeding up the research and development of life-saving new drugs and medical treatments.
  - Improving catalysts that enable petrochemical alternatives or better processes for the carbon breakdown necessary for combating climate-threatening emissions.
  - Providing a speedup for some machine learning problems

Quantum Computing Threats

- Harvest now, Decrypt later



Venona Project

- A United States counterintelligence program initiated during World War II by the United States
- From February 1, 1943, until October 1, 1980
- During the 37-year duration of the Venona project, the Signal Intelligence Service decrypted and translated approximately 3,000 messages.
- Discovery
  - The Cambridge Five espionage ring in the United Kingdom and
  - The Soviet espionage of the Manhattan Project in the US (known as Project Enormous).

National Cyber Security Agency (NCSA)

National Cyber Security Agency (NCSA), Thailand
120 Moo 3, The Government Complex, Building B, 7th Floor,
Chaeng Watthana Road, Thung Song Hong, Lak Si, Bangkok 10210

NCSA Thailand

https://www.ncsa.or.th

saraban@ncsa.or.th

+66 (0) 2 142 6888