ISACA

Belgium Chapter

ACCREDITED TRAINING ORGANISATION

Navigating Privacy in the Age of Generative AI: Challenges and Opportunities for CDPSE and CISM Professionals in Europe

Geert Nobels

ISACA Belgium New Year 2025

PERSONAL BACKGROUND

- Teacher by training (English, **history** and business economics)
- Accredited APMG Trainer for CISM, CISA and CDPSE certifications (ISACA)
- Co-founder / owner of SOCRAI / Genoly.biz (Human cybersecurity)
  - Consulting services on NIS2, ISO27001, GDPR
  - Awareness training for board and employees

- E-mail: geert@socrai.com / 0478 97 33 38
- https://www.linkedin.com/in/geertnobels

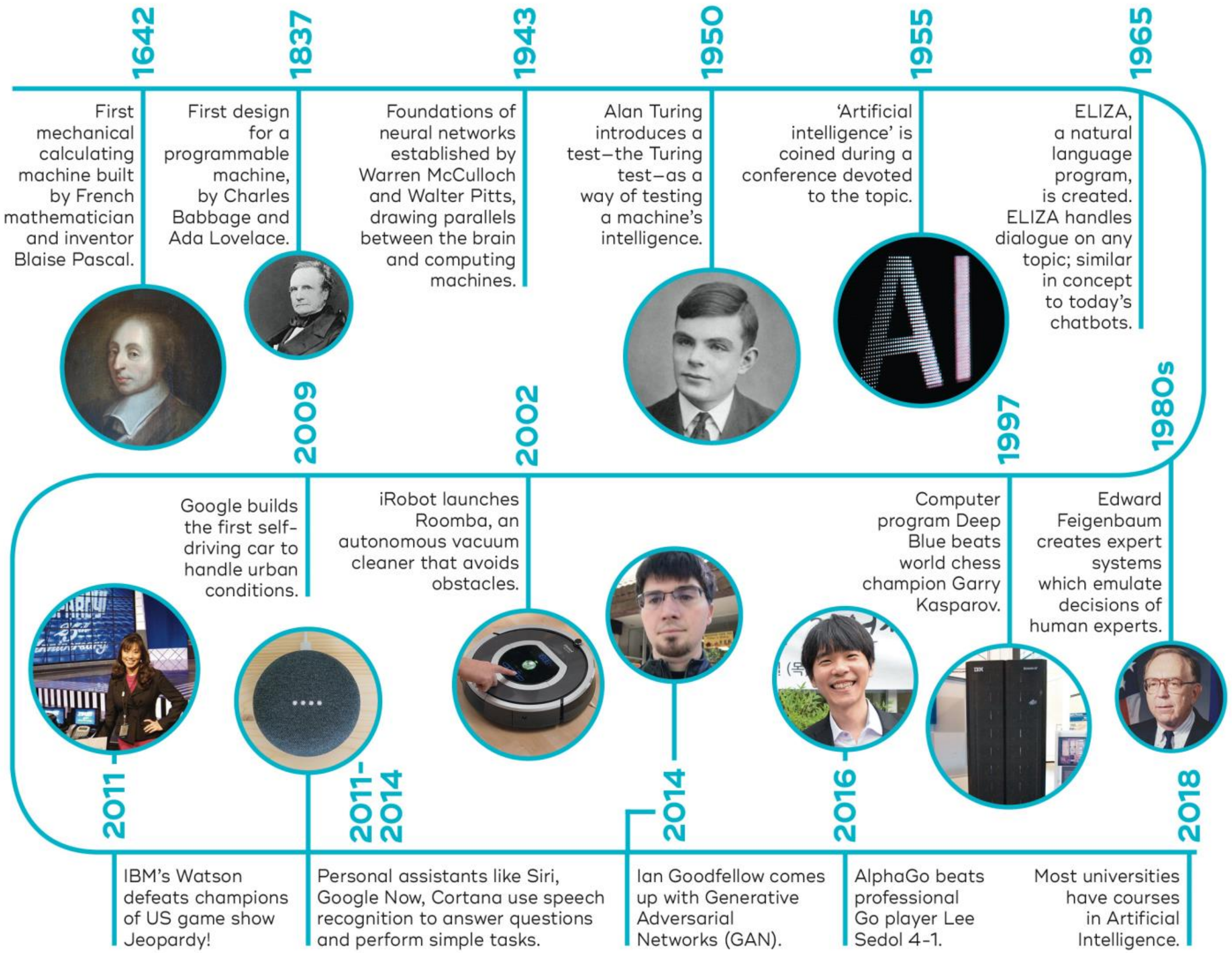
SOCRAI HUMAN CYBERSECURITY

ISACA Belgium Chapter ACCREDITED TRAINING ORGANISATION

TOPICS

- ➢Gen AI
- ➢AI Act
- ➢Shadow IT
- ➢Opportunities for CISM and CDPSE
- ➢Challenges for CISM and CDPSE
- ➢GenAI inside CISM
- ➢GenAI inside CDPSE

GEN AI



1642 First mechanical calculating machine built by French mathematician and inventor Blaise Pascal.

1837 First design for a programmable machine, by Charles Babbage and Ada Lovelace.

1943 Foundations of neural networks established by Warren McCulloch and Walter Pitts, drawing parallels between the brain and computing machines.

1950 Alan Turing introduces a test—the Turing test—as a way of testing a machine's intelligence.

1955 'Artificial intelligence' is coined during a conference devoted to the topic.

1965 ELIZA, a natural language program, is created. ELIZA handles dialogue on any topic; similar in concept to today's chatbots.

1980s Edward Feigenbaum creates expert systems which emulate decisions of human experts.

1997 Computer program Deep Blue beats world chess champion Garry Kasparov.

2002 iRobot launches Roomba, an autonomous vacuum cleaner that avoids obstacles.

2009 Google builds the first self-driving car to handle urban conditions.

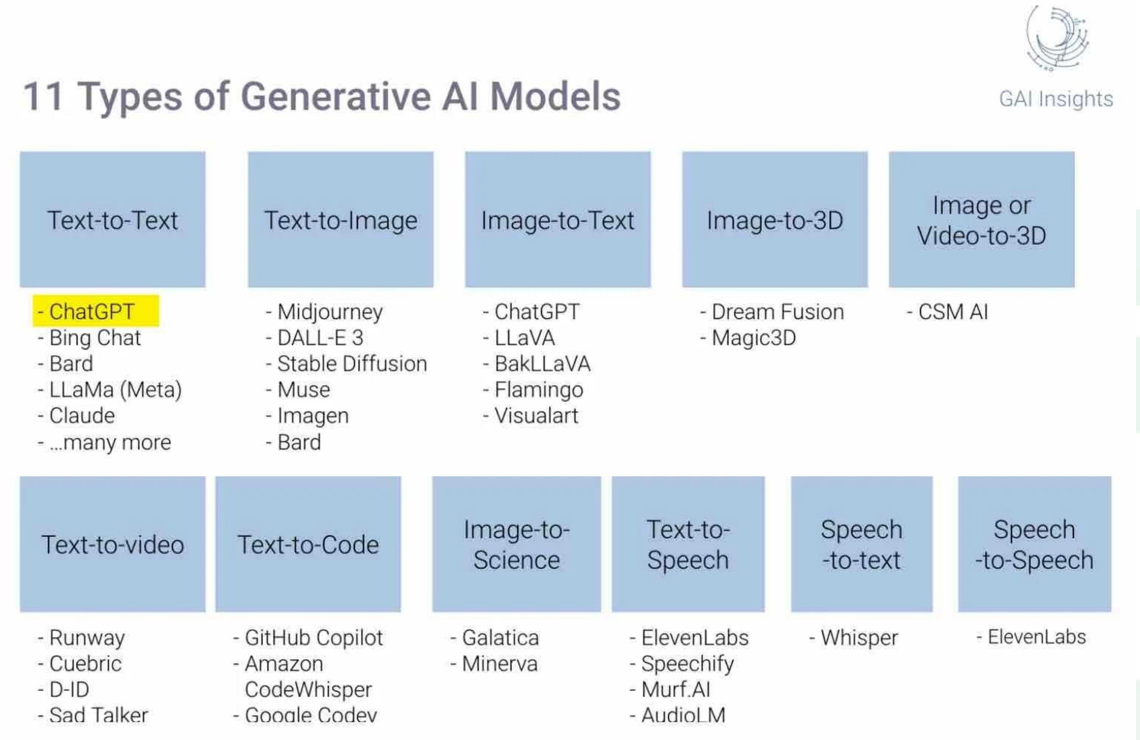
2011 IBM's Watson defeats champions of US game show Jeopardy!

2011-2014 Personal assistants like Siri, Google Now, Cortana use speech recognition to answer questions and perform simple tasks.

2014 Ian Goodfellow comes up with Generative Adversarial Networks (GAN).

2016 AlphaGo beats professional Go player Lee Sedol 4-1.

2018 Most universities have courses in Artificial Intelligence.



11 Types of Generative AI Models

GAI Insights

Text-to-Text
- ChatGPT
- Bing Chat
- Bard
- LLaMa (Meta)
- Claude
- ...many more

Text-to-Image
- Midjourney
- DALL-E 3
- Stable Diffusion
- Muse
- Imagen
- Bard

Image-to-Text
- ChatGPT
- LLaVA
- BakLLaVA
- Flamingo
- Visualart

Image-to-3D
- Dream Fusion
- Magic3D

Image or Video-to-3D
- CSM AI

Text-to-video
- Runway
- Cuebric
- D-ID
- Sad Talker

Text-to-Code
- GitHub Copilot
- Amazon CodeWhisper
- Google Codev

Image-to-Science
- Galatica
- Minerva

Text-to-Speech
- ElevenLabs
- Speechify
- Murf.AI
- AudioLM

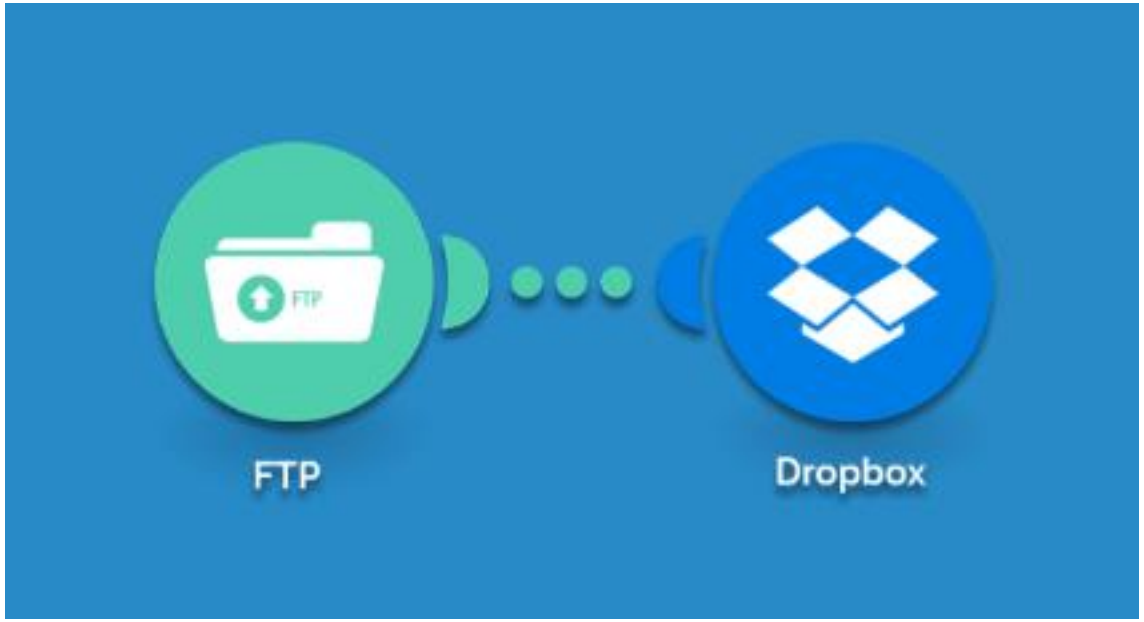
Speech-to-text
- Whisper

Speech-to-Speech
- ElevenLabs

AI ACT (EU’S SAFETY MANUAL FOR AI)

- **What?** The European AI Act is a law in the European Union to regulate how AI (artificial intelligence) is built and used. The goal is to ensure AI is safe, trustworthy, and respects people’s rights.
- **How?** The law divides AI into four levels of risk—just like ranking activities based on how dangerous they can be:
  - Unacceptable Risk (Banned)
  - High Risk (Strict Rules)
  - Limited Risk (Transparency Required)
  - Minimal Risk (No Specific Rules)
- **Impact?** If a company wants to use AI in the EU:
  - They need to know what risk level their AI falls into.
  - If they’re using high-risk AI, they’ll need to document everything, show that they’re testing it for safety, and let people know how decisions are made.
  - For banned AI, companies can’t use it at all.

SHADOW IT



OPPORTUNITIES

CISM

- **Governance and Strategy Development**
  - Policy Drafting Assistance
  - Security Maturity Assessment
  - Risk Framework Development
- **Risk Management and Threat Forecasting**
  - Risk Scenario Generation
  - Threat Landscape Analysis
  - Predictive Analysis
- **Security Operations and Incident Response**
  - Incident Response Playbooks
  - Post-Incident Reporting
  - Root Cause Analysis
- **Compliance and Audits**
  - Compliance Reports
  - Control Mapping
- **Security Awareness and Communication**
  - Tailored Training Materials
  - Management Reporting

CDPSE

- **Privacy Governance and Compliance**
  - Privacy Impact Assessments (PIAs)
  - Regulatory Research Summarization
  - Policy Generation:
- **Privacy Architecture Design**
  - Data Flow Mapping
  - Anonymization and Synthetic Data
  - Privacy-by-Design Templates
- **Data Lifecycle Management**
  - Data Classification
  - Data Retention Policies
  - Automated Data Deletion
- **Data Subject Rights and Transparency**
  - DSAR (Data Subject Access Request) Automation
  - Consent Management
  - Breach Notifications

ISACA Belgium Chapter
ACCREDITED TRAINING ORGANISATION

CHALLENGES

CISM

- **Security and Risk Management Challenges**
  - New Attack Vectors
  - Data Leakage Risks
  - Limited Security Controls.
- **Governance and Accountability Issues**
  - Lack of Transparency
  - AI Misuse and Shadow IT
  - Vendor Risks
- **Incident Response and Threat Detection**
  - Synthetic Threats
  - Increased Incident Complexity

CDPSE

- **Privacy and Data Management Concerns**
  - Unintentional Use of Personal Data
  - Data Minimization
  - Synthetic Data Risks
- **Compliance and Regulatory Risks**
  - Regulatory Gaps:
  - Data Subject Rights (DSRs):.
  - Cross-Border Data Transfers:
- **Consent and Transparency Issues**
  - Lack of Explainability:.
  - Informed Consent:

ISACA Belgium Chapter
ACCREDITED TRAINING ORGANISATION

GEN AI AND CISM

- **Information Security Governance**
  - Establishing governance frameworks to ensure ethical and compliant use of GenAI technologies.
  - Addressing AI-specific risks like data privacy, misuse of AI-generated content, and ethical concerns.
  - Ensuring that GenAI tools align with regulatory and industry standards.
  - Defining acceptable use policies for AI-generated content
- **Information Risk Management**
  - Identifying risks specific to GenAI, such as data poisoning, model theft, or misuse of synthetic data.
  - Conducting risk assessments to understand how GenAI systems impact confidentiality, integrity, and availability (CIA).
  - Evaluating risks associated with bias in models and potential intellectual property (IP) exposure.
  - Implementing controls to mitigate GenAI risks, such as protecting APIs and training data sources.
- **Information Security Program Development and Management**
  - Integrating GenAI-specific controls into the broader security program.
  - Managing access controls for GenAI systems, ensuring that only authorized personnel can use, modify, or deploy AI models.
  - Developing training programs to educate stakeholders about the risks and proper use of GenAI.
  - Defining policies for lifecycle management, including data used to train models and processes for updating models securely.
- **Information Security Incident Management**
  - Creating incident response plans for GenAI-related incidents, such as misuse of AI-generated outputs or compromise of AI infrastructure.
  - Implementing monitoring for unusual activity in GenAI models (e.g., excessive API requests or unauthorized attempts to train/deploy models).
  - Establishing processes to mitigate the effects of "hallucinations" or incorrect outputs in critical business contexts.
  - Managing post-incident reviews to understand the root cause and prevent recurrence of GenAI-related incidents.

GEN AI AND CDPSE

- **Provacy Governance**
  - Establishing governance policies for the ethical and compliant use of GenAI tools (e.g., GPT models or internal AI assistants).
  - Ensuring compliance with GDPR, CCPA, HIPAA, or other regulations related to data used for training and inference in GenAI systems.
  - Defining roles and responsibilities for GenAI system oversight to ensure accountability for privacy-related AI incidents.
  - Establishing frameworks for privacy impact assessments (PIAs) when deploying GenAI models, especially when they process personally identifiable information (PII).
  - Defining ethical guidelines for data minimization in Generative AI training data to avoid unnecessary exposure of private information.
- **Privacy Architecture**
  - Designing privacy-aware AI architectures that prevent sensitive data from being unintentionally exposed through training or outputs.\n
  - Implementing differential privacy techniques and synthetic data generation to protect the privacy of data used for training GenAI models.
  - Encrypting and pseudonymizing sensitive data inputs and outputs in GenAI APIs to ensure data privacy in transit and at rest.
  - Ensuring that GenAI model outputs do not inadvertently leak PII by developing post-processing filters for outputs.\n
  - Integrating data retention policies into GenAI systems to automatically delete training data after the model lifecycle requirements are met.
- **Data Lifecycle**
  - Ensuring that the data collection process for training and fine-tuning GenAI models adheres to consent and purpose limitations.\n
  - Implementing controls to avoid the use of real personal data when unnecessary by opting for synthetic or anonymized data.\n
  - Defining retention and deletion policies to ensure that personal data used for AI training or testing is deleted after use.\n
  - Auditing the data sources used for training GenAI models to ensure that no unlawful or unauthorized data is included.\n
  - Managing the data sharing processes in GenAI systems to ensure that third-party data usage (for APIs or plug-ins) adheres to privacy agreements.\n

THANKS FOR YOUR ATTENTION

ISACA
Belgium Chapter
ACCREDITED TRAINING ORGANISATION

ISACA
Belgium Chapter
ACCREDITED TRAINING ORGANISATION

FOLLOW US FOR MORE UPDATES

Instagram

LinkedIn