AI in Cybersecurity:

Harnessing its Power for Protection, Guarding Against its Threats

Presented By: Tina Lampe

Discussion Points:

1. AI Level Set
2. Harnessing the Power of AI
3. Adversary Amplification with AI
4. Ethical and Privacy Considerations
5. The Near-Term Future
6. Key Actions

1. AI Level Set:
    * Generative AI
    * Large Language Models (LLMs)
    * Agentic AI

GenAI, LLMs , Agentic AI – What's the Difference?

Gen AI	LLMs	Agentic AI
Can **Generate** new content such as text, images, music, code, video	Large Language Models (LLMs) are advanced machine learning models designed to **understand and generate human language.**	Also called Autonomous AI or Self-directed AI – is **proactive** without constant human guidance
Reactive – waits for input before creating something new	Humans interact with Large Language Models (LLMs) using **Prompts** - LLMs will process and generate language or ideas based on these prompts	Operates **autonomously** (makes decisions, executes actions, perceives then **adapt**s to environment changes, processes information, generates outputs) to **achieve specific goals**
Test Output Quality - by validating output based on input request	Techniques to interact may involve **prompt engineering** and **RAG** (retrieval-augmented generation)	**Test Output Quality** – by focusing on objectives, constraints and oversight mechanisms.
	Test Output Quality - by validating output based on input request	

AI Agents –vs- Agentic AI

AI Agents	Agentic AI
➢ **Example**: Chatbots for customer support, simple anomaly detection systems	➢ **Example**: Autonomous threat hunting systems, adaptive defense mechanisms
➢ **Specialized** AI programs designed for specific tasks	➢ Advanced AI systems with a degree of **autonomy**
➢ Operate within **predefined** parameters	➢ Can make **independent decisions** and **take actions**
➢ **React to inputs** based on programmed rules	➢ Learns and **adapts** to new situations
➢ **Limited** autonomy and decision-making capability	➢ Operates **across multiple domains** and tasks
	➢ **Collaborates** with other AI systems **and humans**

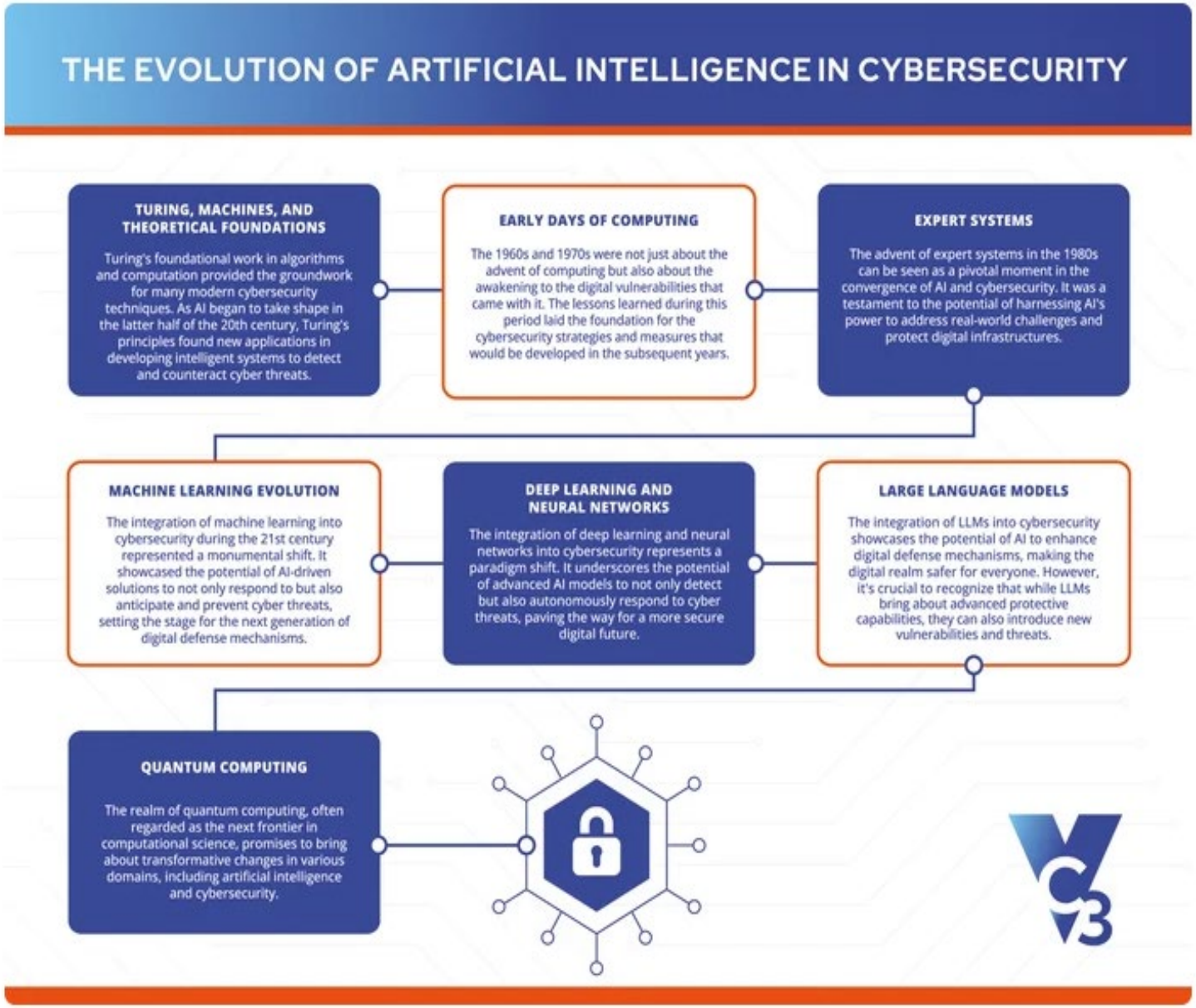
Source: https://right-hand.ai/blog/agentic-ai-in-cybersecurity/

2. Harnessing the Power: AI in Cybersecurity

The AI/Cybersecurity Evolution

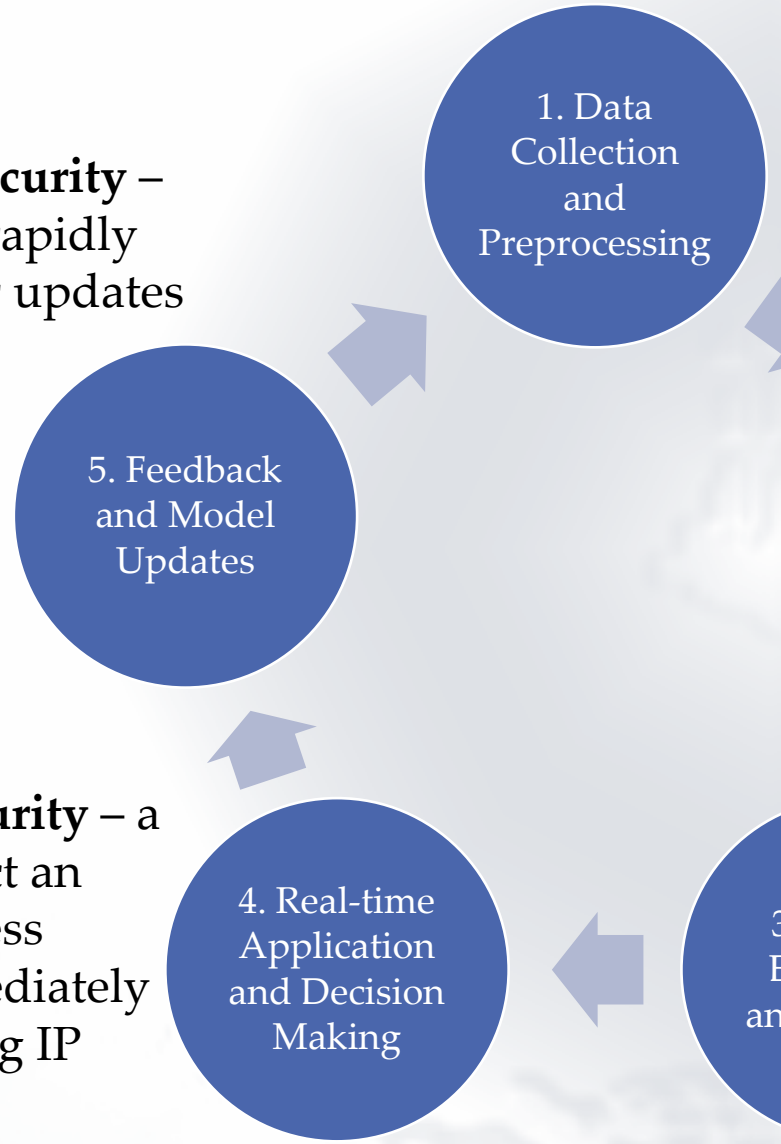
Approx 1980's:
- First computer Virus
- Cybersecurity as a profession

Early 2000's:
- Integration of AI via machine learning into cybersecurity



* Source: vc3 blog

Historic Machine Learning/AI Process



-> 1. For cybersecurity – data includes network traffic logs system activity reports and threat signatures

-> 2. Feed the model data to identify patterns and relationships

-> 3. For cybersecurity – features could include unusual login times, sudden spikes in network activity or irregular file modifications.

-> 4. For cybersecurity – a model could detect an unauthorized access attempt and immediately block the offending IP address

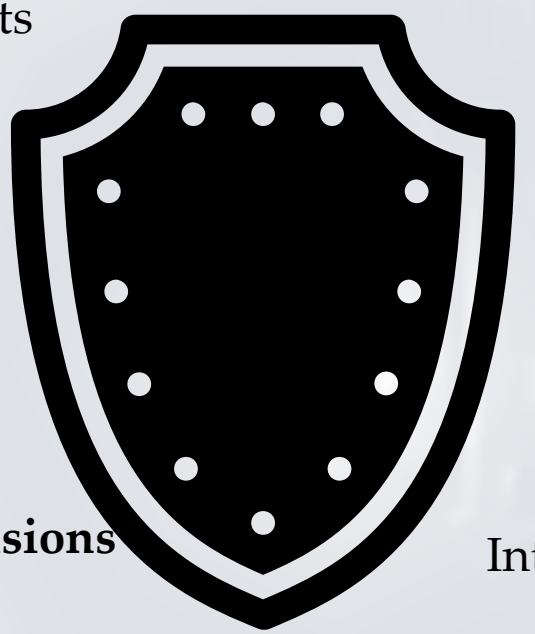
-> 5. In cybersecurity – threats evolve rapidly making regular updates essential

2024 View - AI Enhanced Defense

An Efficient, AI Enhanced SOC
'Finding the needle in the haystack'

Uncover hidden priority threats

Predict future attacks



Real Time Incident Response

Auto-Adapt defense tactics to evolving threats

Behavior Analysis

Zero Trust Architecture Support

Enhanced Human Oversight and Decisions

Intelligent Alert Prioritization

AI Powered Threat Intelligence Platforms
(aggregate and analyze data from various sources)

* Source: analyticsinsight.net

Continuous Improvement: Cybersecurity Machine Learning/AI Use Cases

CyberSecurity Machine Learning Use Cases
➢ Detect and Classify Threats
➢ Detect Anomalies
➢ Detect and Prevent Malware
➢ Intrusion Detection
➢ **Detect Spam and Phishing**
➢ **Endpoint Security**
➢ Network Risk Scoring
➢ Managing Vulnerabilities
➢ **DDoS and Botnet Protection**

More Recently – Cybersecurity Enhanced with GenAI

- Data Masking for Privacy Protection
- Synthetic Malware Generation
- Reporting enhancements
- Secure Code recommendations
- Automated Secure Policy Generation
- Creation of Interactive Cybersecurity Training

2025 – Towards more Agentic AI in Cybersecurity

Security Operations Agentic Use Cases	Application Security Agentic Use Cases
Triage and Investigation	Risk Identification
Adaptive threat hunting	Application test creation and adaptation
Response Actions	**Dynamic application test execution**
Adversary Simulation	**Autonomous Test Case remediation**
Remediate External Exposure	**Automated Pen Testing**

Challenges - Agentic AI

Agentic AI Cybersecurity Implementation Challenges
Lack of transparency and interpretability
Data Quality and Breadth concerns
Maintaining Reliability
Complexity of Implementation
Human Oversight needs

3. Adversary Amplification with AI

AI Lowers the Barrier to Entry for Sophisticated Cyber Attacks

- According to cybersecuritynews.com, “AI-assisted approach significantly lowers the barrier to entry for malicious actors and enables rapid scaling of attacks-even by technically unskilled individuals.”

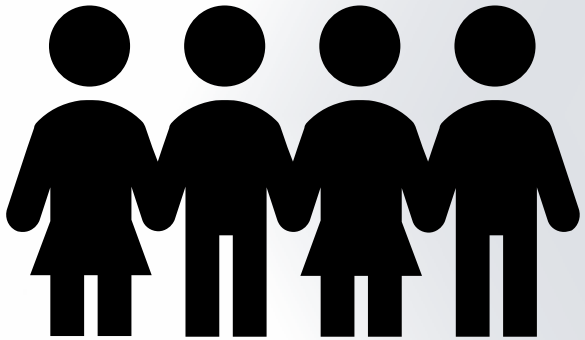
* Source: cybersecuritynews.com

Major AI-Driven Threat Vectors

- Digital Identity
- Recon As A Service -> Attack Blueprint
- LLM Poisoning
- AI Powered Social Engineering
- AI Generated Malware
- Data Mining

4. Ethical and Privacy Considerations

Ethical Considerations



- Privacy –vs- Security
- Bias and Fairness
- Accountability and Decision Making
- Transparency and Explanation

* Source: isc2.org

Trustworthy AI Framework Examples

NIST AI 100-1:

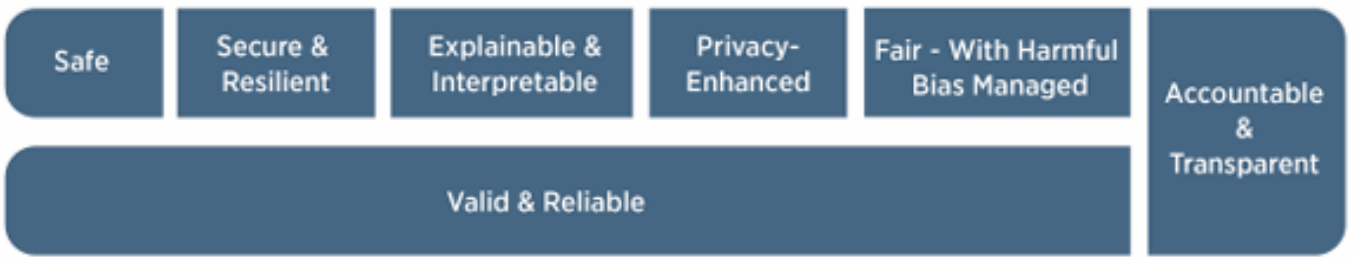


Fig. 4. Characteristics of trustworthy AI systems. Valid & Reliable is a necessary condition of trustworthiness and is shown as the base for other trustworthiness characteristics. Accountable & Transparent is shown as a vertical box because it relates to all other characteristics.

ISO/IEC 42001

What are the main benefits of implementing ISO/IEC 42001?

- **Responsible AI**: ensures ethical and responsible use of artificial intelligence.
- **Reputation management**: enhances trust in AI applications.
- **AI governance**: supports compliance with legal and regulatory standards.
- **Practical guidance**: manages AI-specific risks effectively.
- **Identifying opportunities**: Encourages innovation within a structured framework.

5. The Near-Term Future

AI Becoming more Deeply Integrated into Business Operations

Continued Focus
AI in Cybersecurity

Cyber Resilience and Agility

Targeted Organization Rankings and Remediations Based on Business Impact

Refinement of Cyber Defenses near real time

Freeing the Security Team to work on Strategic Tasks

Scaling Cyber Defense Activities when Needed

Continuous Compliance Assessments

Shifting from Vulnerability-Based to Exploitability-Based Security

6. Key Actions

Key Actions

1. **Confirm** your Organization's AI Cybersecurity Strategy includes Ethical Considerations and Trustworthy AI strategies

2. Continually **Invest** time to stay current on AI Cybersecurity enhancements which are progressing at an exponential pace

3. Stay **vigilant** in protecting your organization's most valuable assets from AI enhanced cyber threats

Questions?

That's a Wrap

Feel Free to Connect with me on LinkedIn:
https://www.linkedin.com/in/tina-lampe

Thanks for your time and insights today!