The interplay of Secure AI and Cyber Security Threat Mitigation

Atlantic Health System

AI is changing the game when it comes to Cybersecurity – for both us and cyber criminals

Atlantic Health System

Sunil Dadlani & Atlantic Health System

- CIO & Executive Vice President at Atlantic Health System since September 2020
- NY Health Information Technology & Health Information Exchange, Advisory Board Member
- Advances Atlantic Health System's use of technology to support delivery of excellent patient care & team member experiences
- Sunil.Dadlani@atlantichealth.org

- Nationally recognized top clinically integrated health system setting standards for quality health care in New Jersey, Pennsylvania & the New York metropolitan area
- 20K+ team members
- Serving 6.2 million people
- 7 large multi-specialty hospitals, 500 sites of care,

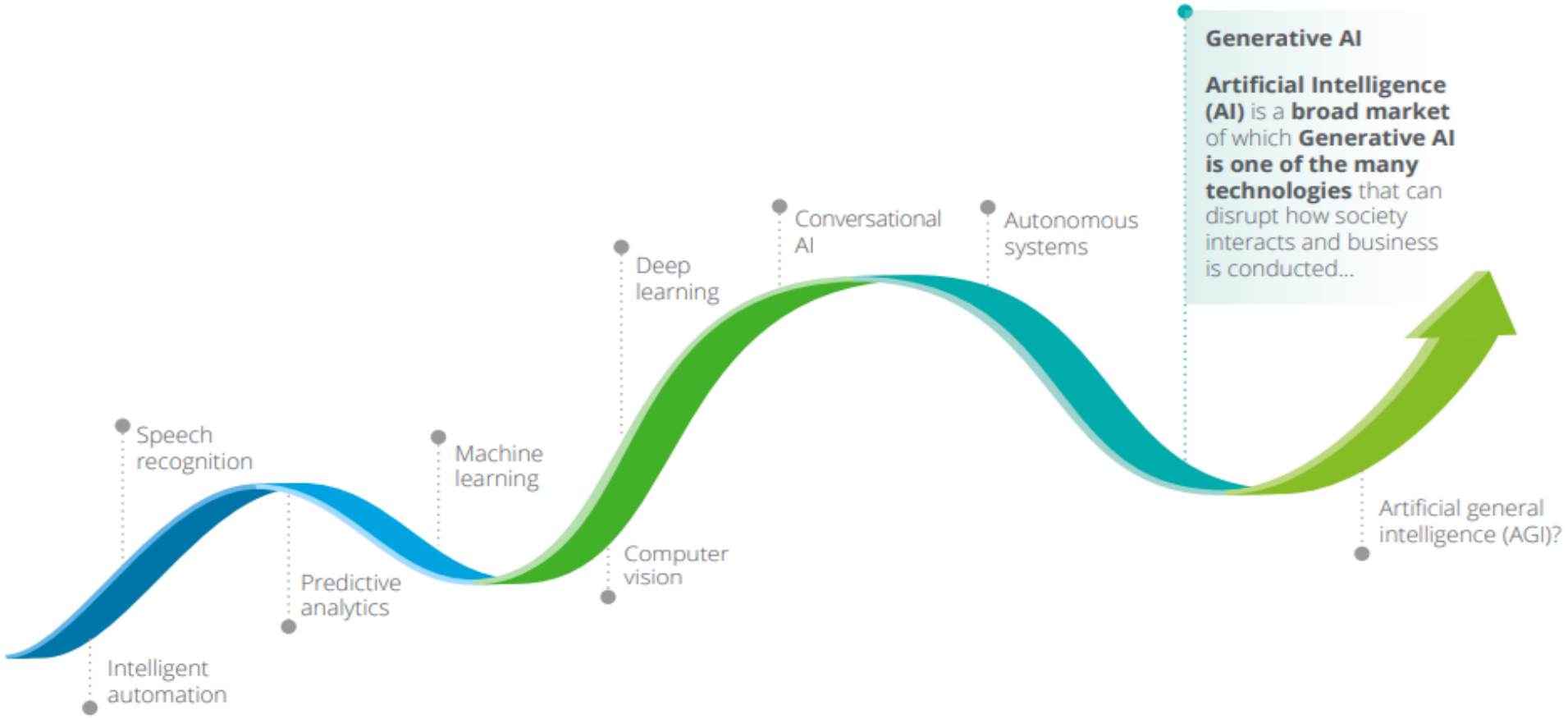
Atlantic Health System

Agenda

- Introduction
- Evolution of AI
- Double Edged Sword of AI
- Using AI as a Defensive Shield
- Ethical Considerations and AI Governance
- Regulatory Impact
- Preparing for the Future
- Q&A

Atlantic Health System

Evolution of AI

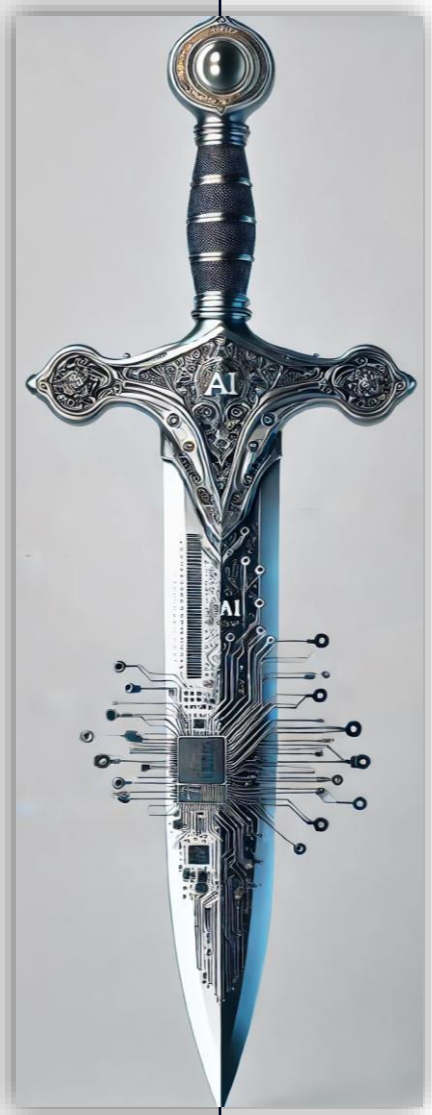


Atlantic Health System

Double Edged Sword of AI

Enhancing Health Systems

- Improving Diagnostics
- Preventive, Personalized Precision Medicine
- Operational Efficiency, Research & Innovation

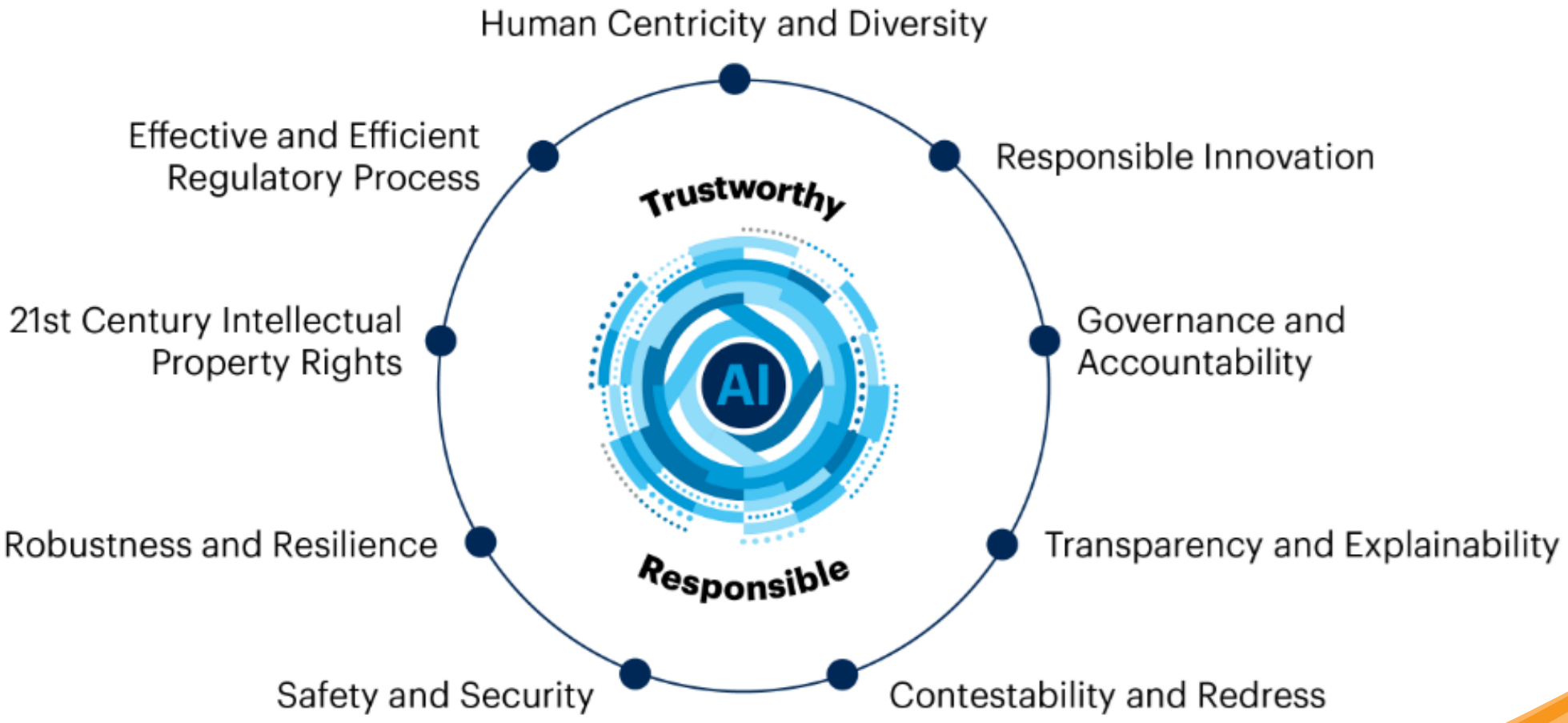


Empowering Cyber Criminals

- Advanced Attacks
- Automation of Attacks
- Bias & Inequity, Errors & Misdiagnoses

Atlantic Health System

Trustworthy and Responsible AI (Deloitte Framework)



Atlantic Health System

International Approach to AI

United States

Regulatory Approach:

- The U.S. has a more market-oriented approach, with regulations often developed sector by sector rather than through comprehensive national AI laws.

Privacy and Data Protection:

- While there is no overarching federal privacy law, various states have enacted their own laws (e.g., California Consumer Privacy Act).
- Sector-specific laws, like the Health Insurance Portability and Accountability Act (HIPAA), also impact AI development.

Innovation-Focused:

- U.S. policies often emphasize supporting AI innovation and research, with less focus on restrictive measures.

National Security:

- There are regulations concerning AI in the context of national security and defense.

European Union

Comprehensive Legislation:

- The EU is known for its comprehensive approach to AI regulation, prioritizing ethical standards and human rights.

General Data Protection Regulation (GDPR):

- This regulation significantly impacts AI development, focusing on data protection and privacy.

Risk-Based Approach:

- The proposed AI Act categorizes AI systems based on their risk level, imposing stricter regulations on 'high-risk' AI systems.

Focus on Transparency and Accountability:

- The EU emphasizes the need for transparency in AI algorithms and the ability to hold developers accountable.

China

State-Led Development:

- The Chinese government plays a significant role in the development and regulation of AI, with an emphasis on becoming a world leader in AI technology.

National Strategies:

- China has comprehensive plans for AI, including setting targets for the industry's growth and applications in various sectors.

Surveillance and Security:

- There's a significant focus on using AI for surveillance and security, leading to different regulatory considerations compared to the US and EU.

Data Privacy Laws:

- China has introduced data privacy laws (e.g., Personal Information Protection Law), but the approach to data privacy can be different from Western models, with a focus on state security and social stability.

Atlantic Health System

Security by Design, by Default and by Demand

Security by Design

Integrating security measures into the AI development process from the ground up, rather than adding them as an afterthought.

- **Purpose**: Ensures that AI systems are built with strong security foundations, reducing vulnerabilities and potential risks.
- **Implication**:
  - Shifts accountability to AI developers and companies, ensuring that security is a priority from the start.
  - Encourages comprehensive threat modeling and risk assessment throughout the development lifecycle.

Security by Default

AI systems should be secure out of the box, with security settings enabled by default, requiring minimal user intervention to maintain security.

- **Purpose**: Protects users who may not have the expertise to configure security settings properly, ensuring a safer baseline.
- **Implication**:
  - Holds tech companies accountable for delivering inherently secure AI products.
  - Limits the chances of security misconfigurations, reducing the attack surface.

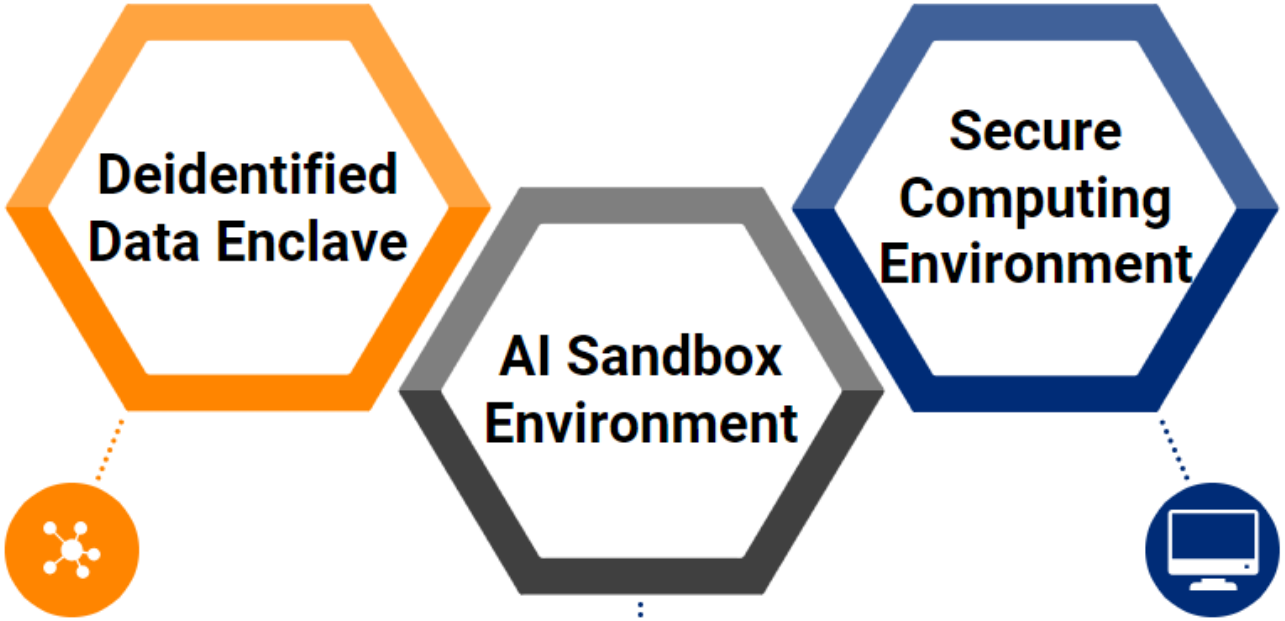
Security by Demand

Reflects the growing expectation from consumers and businesses that AI solutions must meet high security standards as a default expectation.

- **Purpose**: Pushes tech giants and AI startups to prioritize security due to consumer pressure and demand.
- **Implication**:
  - Drives market competition on the basis of security, leading to better, more secure AI products.
  - Increases transparency and responsiveness from tech companies to address security concerns.

Atlantic Health System

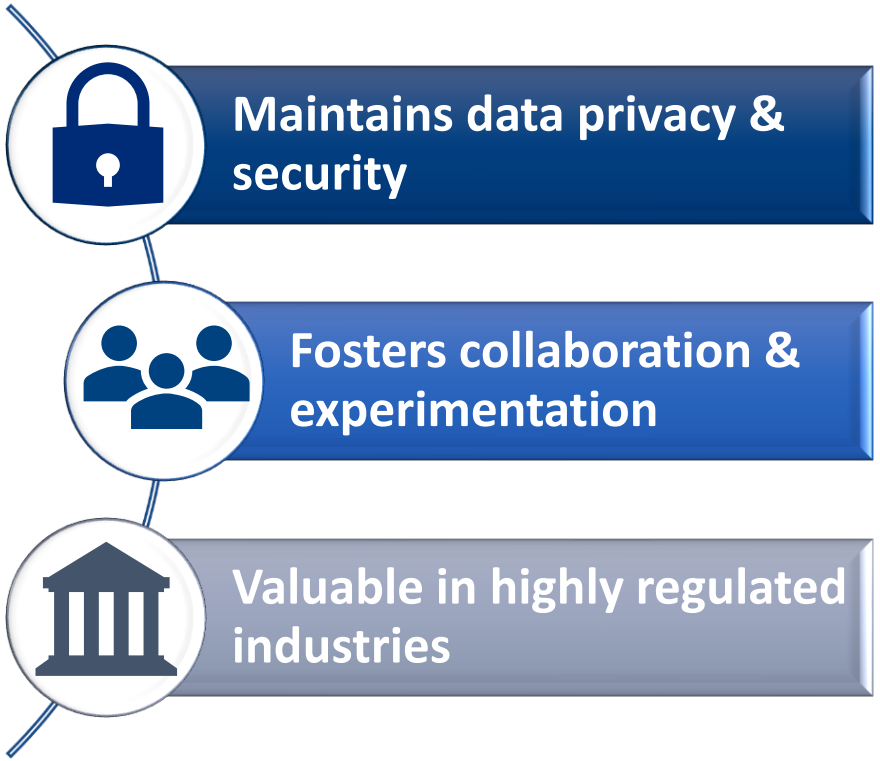
Secure AI Testing Solutions



- A secure and isolated environment where sensitive data is stored and processed

- A controlled and secure space where organizations can test AI models and applications without putting sensitive or real data at risk

- Provides a secure computing environment with restricted internet access, preventing data leaks or breaches



*These **are not foolproof** and **require rigorous governance, access controls, and monitoring to mitigate risks.***

Atlantic Health System

Types of Attacks

Data Poisoning

Adversarial attacks on AI training data in medical imaging)

Model Inversion Attacks

Extracting sensitive patient data from AI models

Adversarial Attacks

Slight alterations in medical images causing misdiagnosis

Social Engineering

AI chatbots manipulated to disclose patient information

System Disruptions

Ransomware attacks impacting AI-integrated systems like Patient Portals

Results in potential

- **Privacy Concerns**
- **Bias & Inequality**
- **Medical Errors / Misdiagnoses**
- **Reduction in Trust**

Atlantic Health System

AI, Gen AI, GAN In Enhancing Cyber Defense

Real-Time Monitoring

AI can monitor endpoint behavior to detect and respond to anomalous activities, such as unauthorized file access or unusual network connections. When such activities are detected, AI can automatically initiate countermeasures, such as isolating the endpoint from the network or rolling back changes made by the malware.

Threat Hunting

AI can assist in proactive threat hunting by scanning for indicators of compromise (IOCs) across the network. This allows cybersecurity teams to identify and neutralize threats before they can cause significant harm.

Ai can analyze historical data and threat intelligence and predict future attacks.

Rapid Response to Threats

GenAI can be used to automate the incident response process, enabling faster and more efficient reactions to detected threats. Once a threat is identified, GenAI can autonomously execute pre-defined response strategies, such as isolating affected systems, blocking malicious IP addresses, or deploying patches.

Threat Simulation and Training

Adversarial Simulations: GenAI can create realistic simulations of cyber attacks, allowing organizations to test their defenses against sophisticated threats. These simulations help identify vulnerabilities in existing security measures and provide insights into how attackers might exploit them.

GAN

Synthetic Data for Training: GANs can generate synthetic data that closely mimics real-world data, providing cybersecurity systems with more diverse training datasets. This can improve the accuracy and robustness of AI models in detecting threats, especially when real data is scarce or sensitive.

.

Adversarial Defense

GANs can be used to strengthen AI models against adversarial attacks by training them on adversarially generated data. This process, known as adversarial training, helps AI systems learn to recognize and resist attempts to deceive them with manipulated inputs.

.

Security Orchestration, Automation, and Response

(SOAR):**Automating Routine Tasks:** AI can automate routine cybersecurity tasks, such as log analysis, vulnerability scanning, and patch management. This frees up human analysts to focus on more complex threats and strategic planning.

.

Coordinated Response

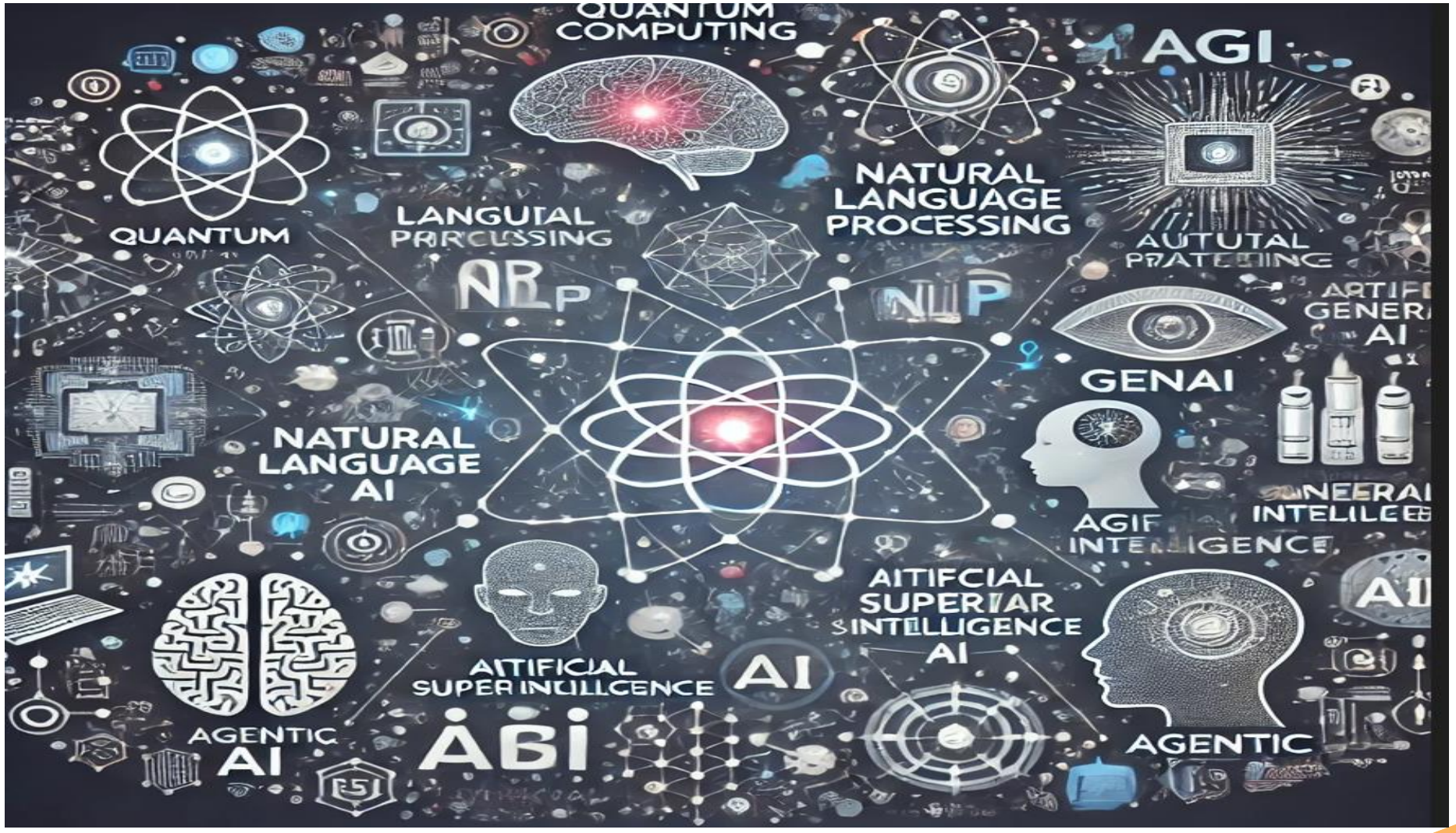
AI can orchestrate a coordinated response to cyber threats by integrating with various security tools and systems. For example, AI can automatically update firewall rules, activate intrusion prevention systems, and notify relevant stakeholders based on the severity of the threat.

Adaptive Defense Mechanisms:

Dynamic Defense Strategies: AI can adapt defense strategies in real-time based on the evolving threat landscape. By analyzing incoming threat data and adjusting security configurations accordingly, AI ensures that defenses are always optimized to counter the most current threats.

Atlantic Health System

Preparing for the future



Atlantic Health System

Questions?

Atlantic
Health System