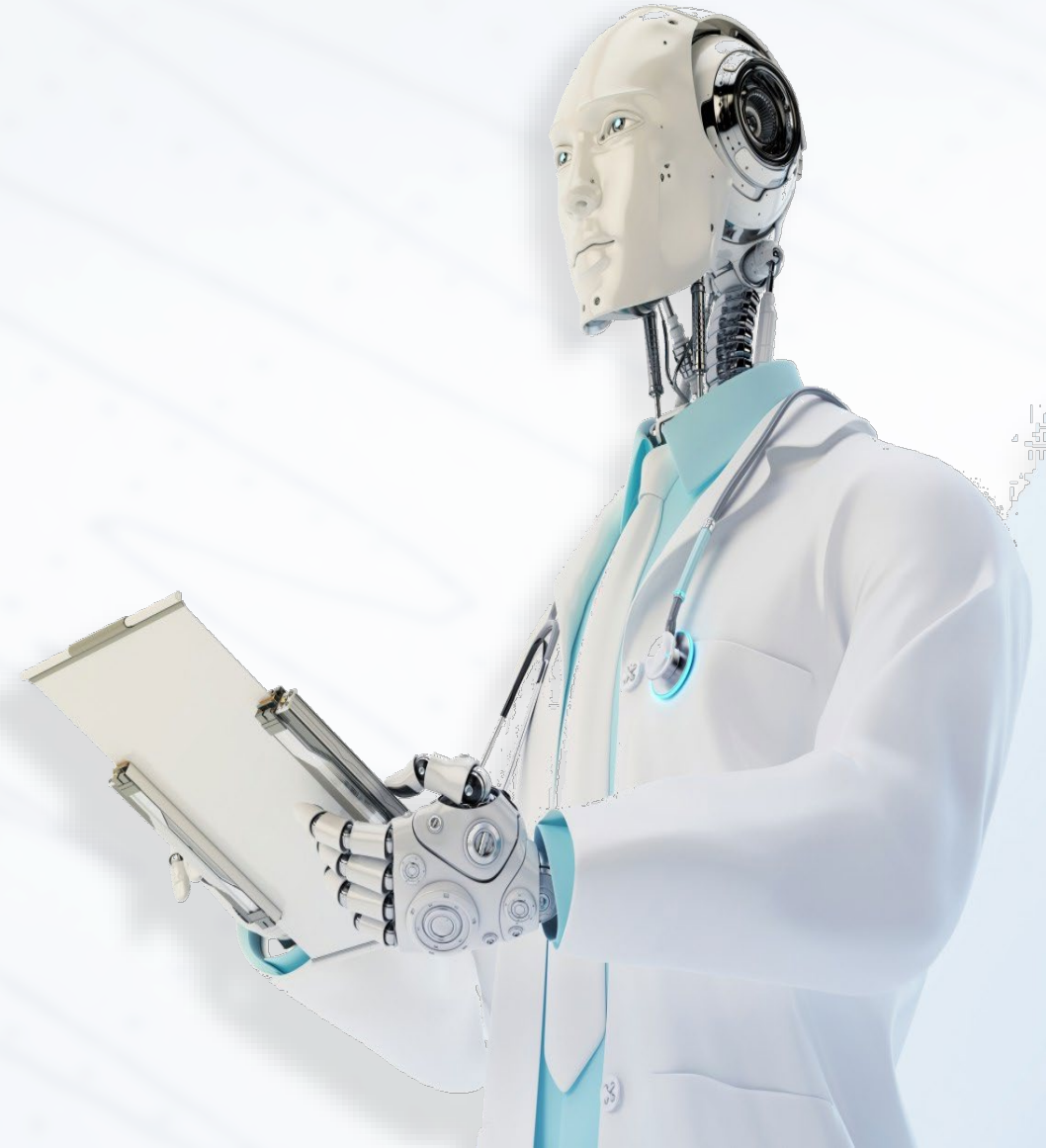


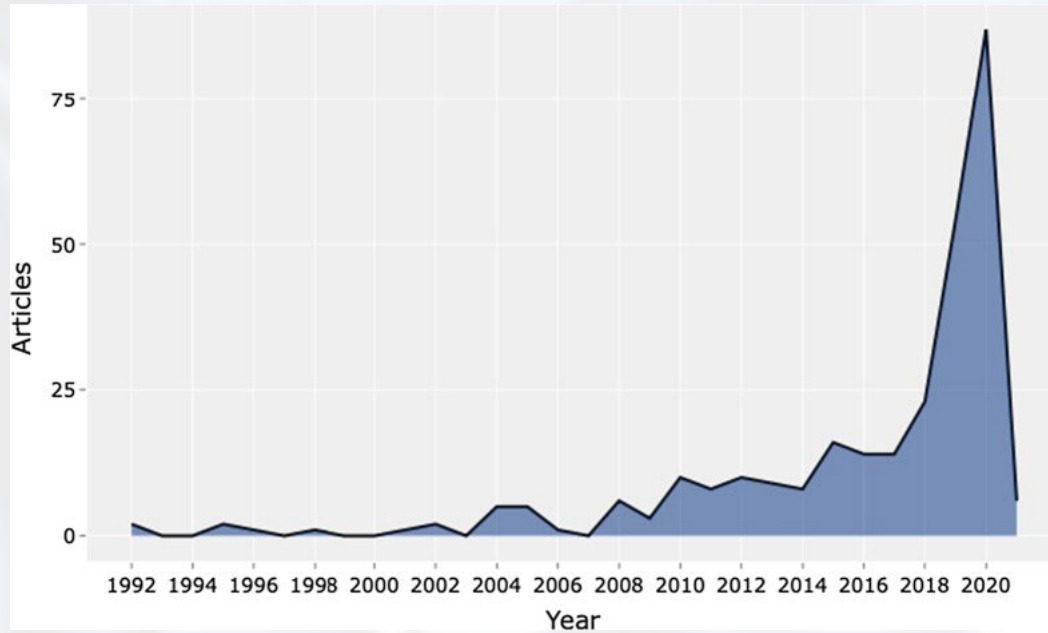
AI in Healthcare

Isabel Praça

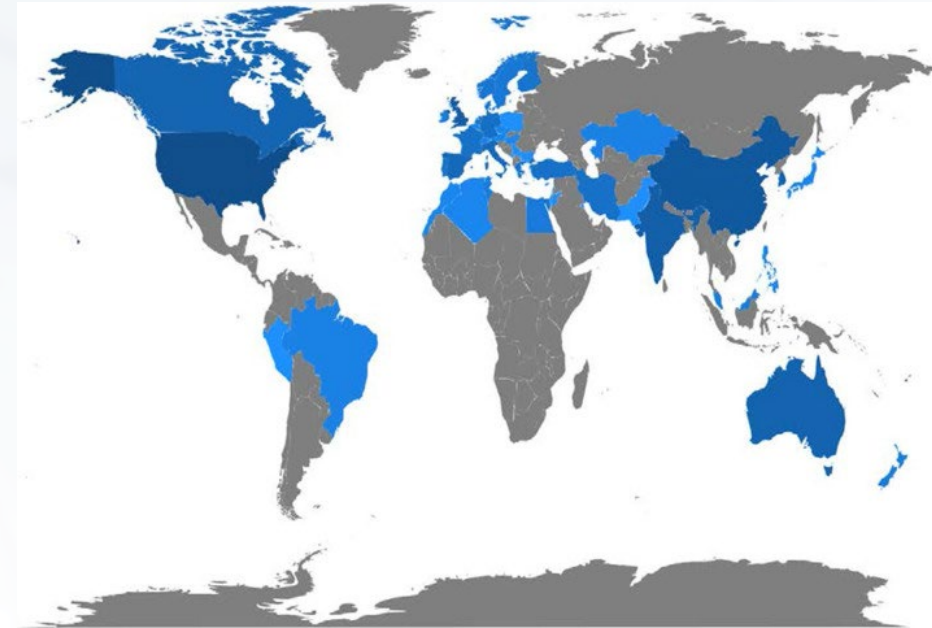
*School of Engineering of the Polytechnic of Porto
Portugal*



Research of AI in Healthcare



Published AI related articles per year.



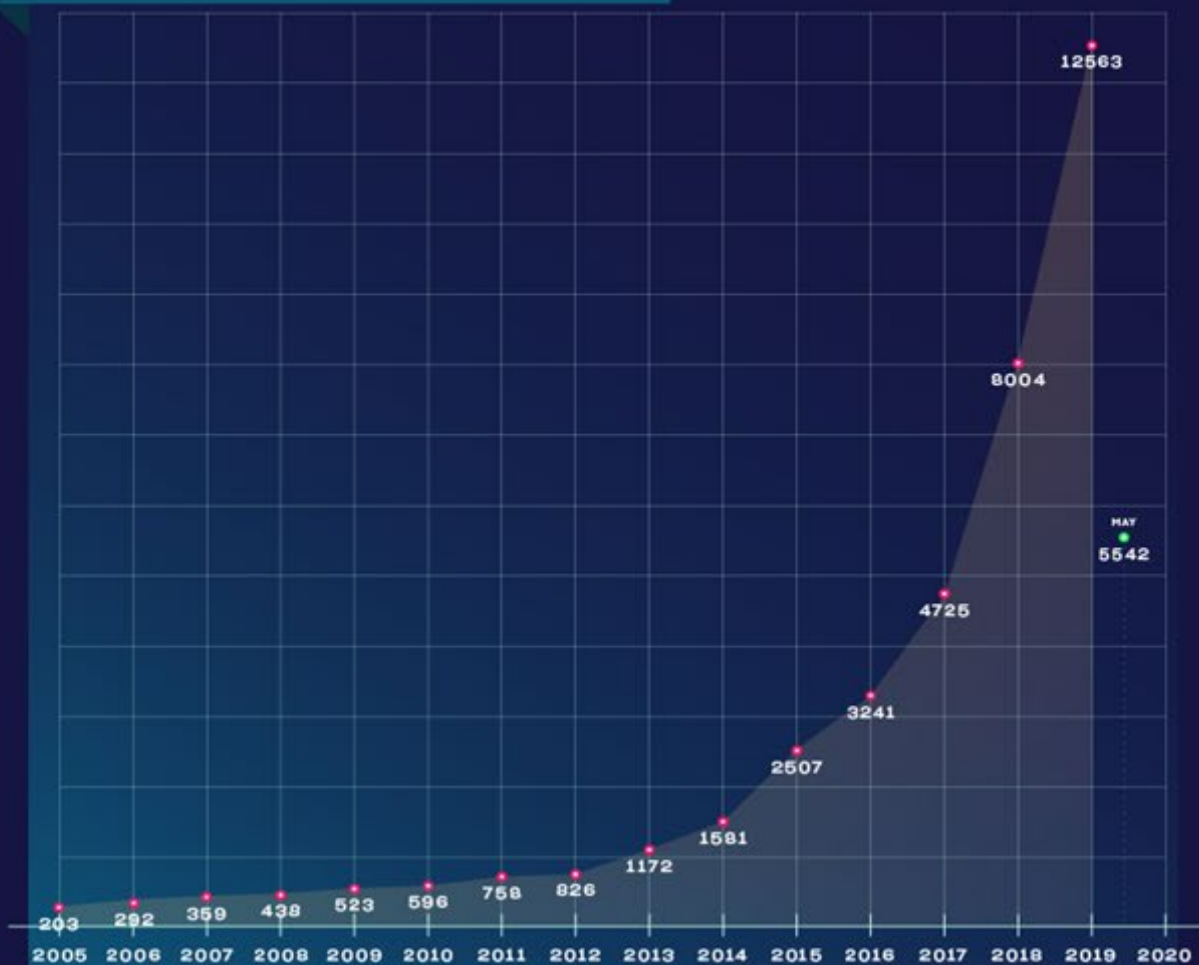
Published AI related articles per country.



a

MACHINE AND DEEP LEARNING STUDIES ON PUBMED.COM

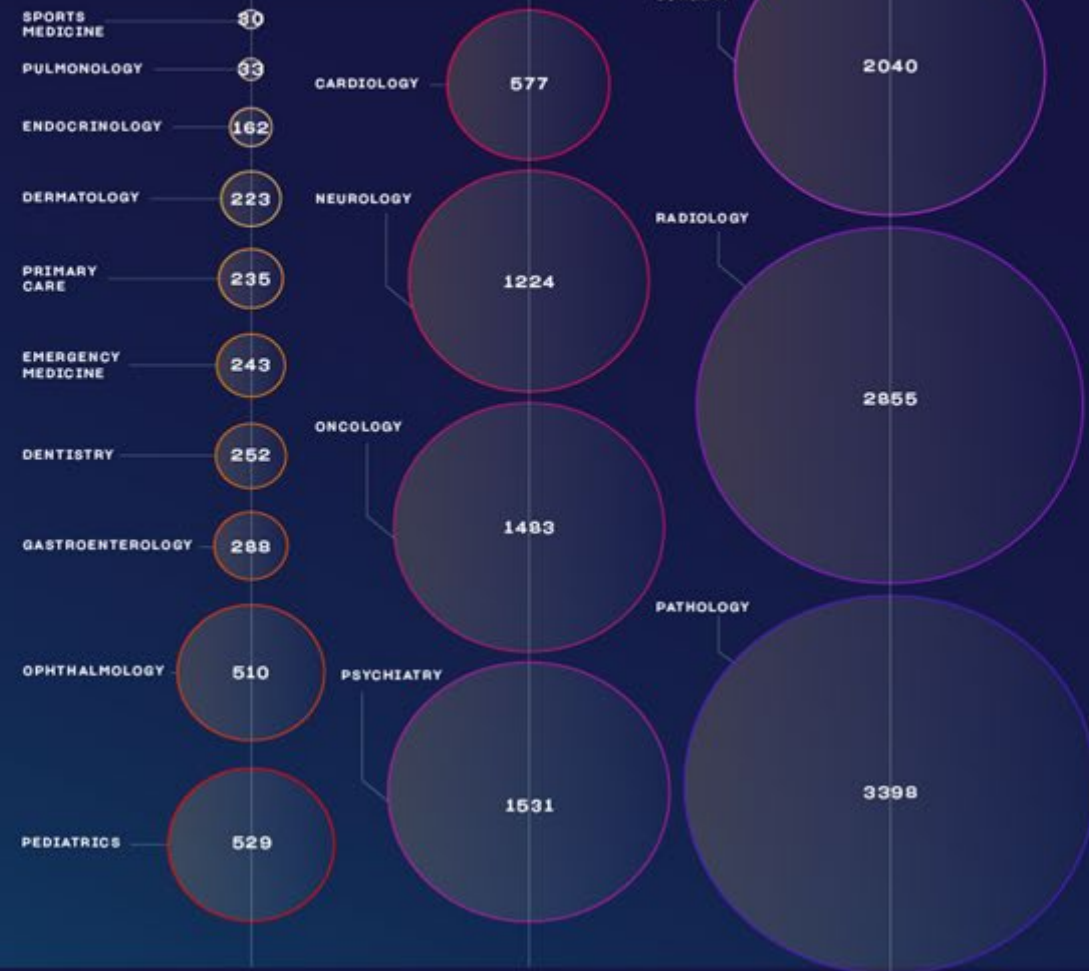
TOTAL NUMBER OF STUDIES



The number of studies found on Pubmed.com using the search term “machine learning” OR “deep learning” and choosing a year in advanced search.

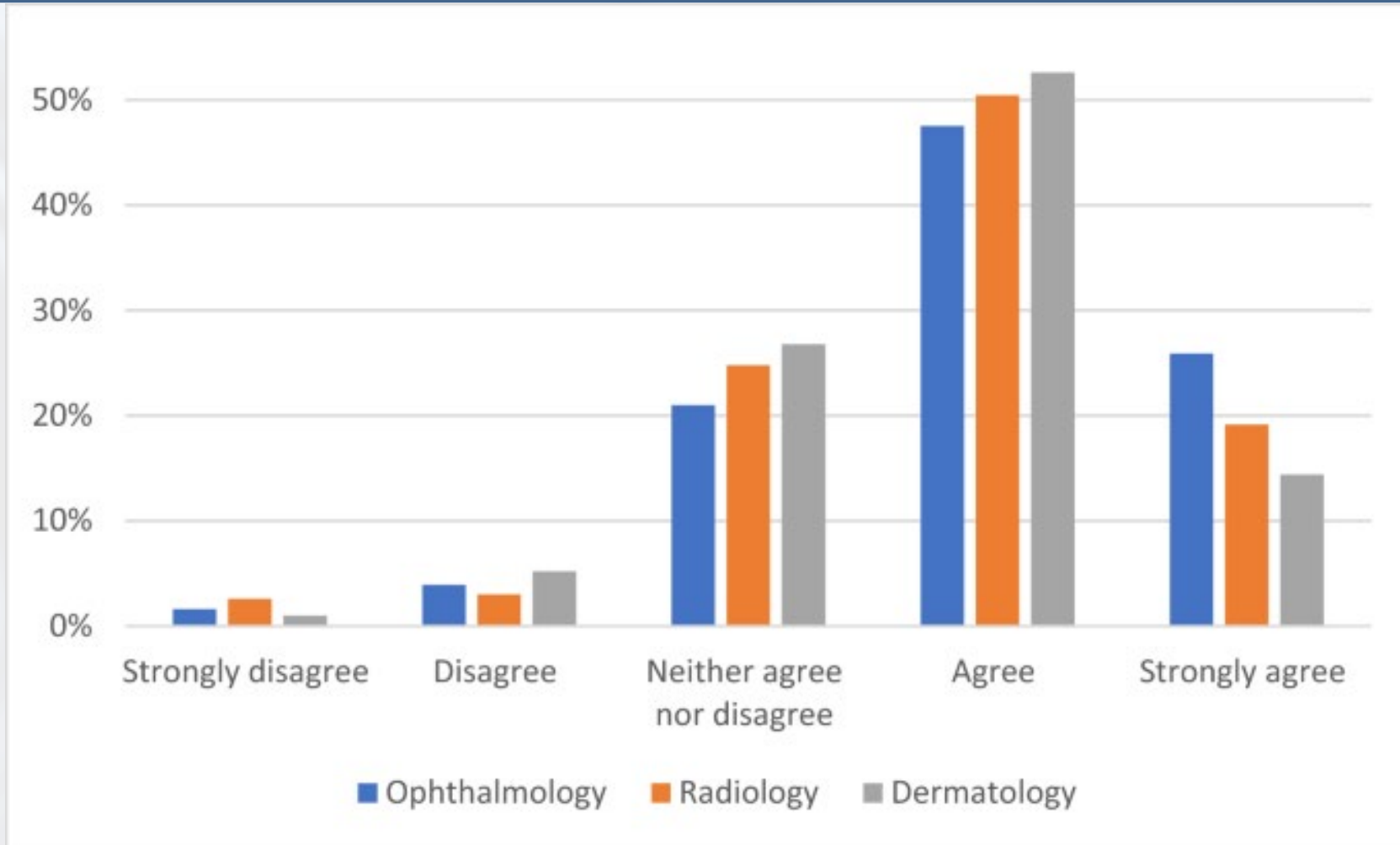
b

STUDIES PER SPECIALTY

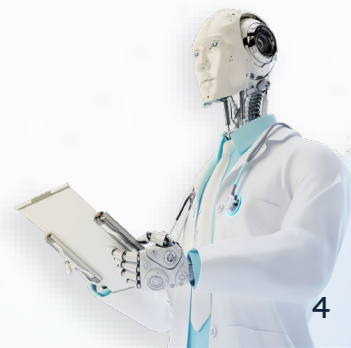


The same search method was used followed by (AND specialty) without specifying a time frame. The number in the circles is the number of studies.

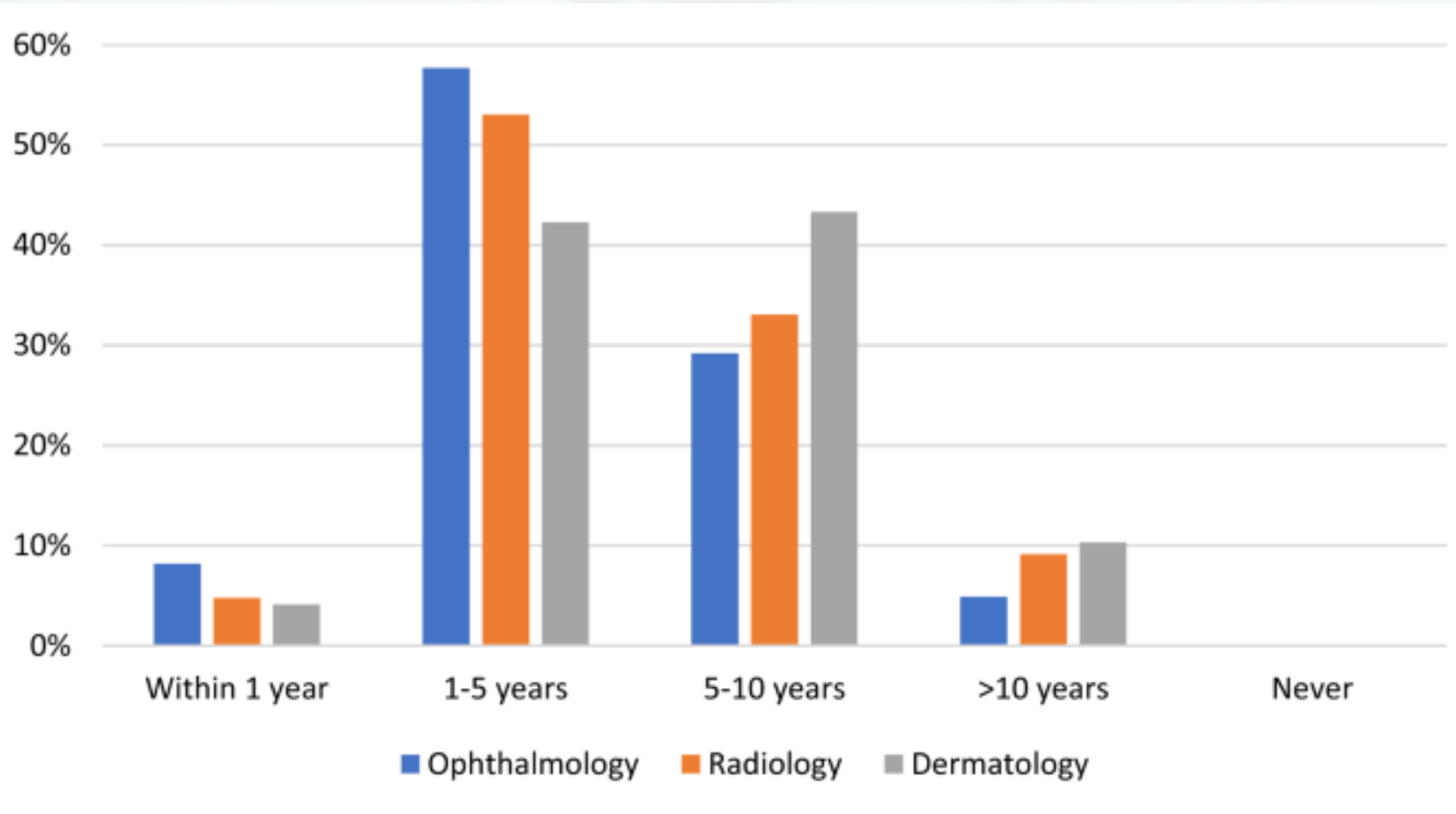
Survey: will your field improve with the use of AI?



Scheetz, J., Rothschild, P., McGuinness, M. et al. A survey of clinicians on the use of artificial intelligence in ophthalmology, dermatology, radiology and radiation oncology. *Sci Rep* 11, 5193 (2021)



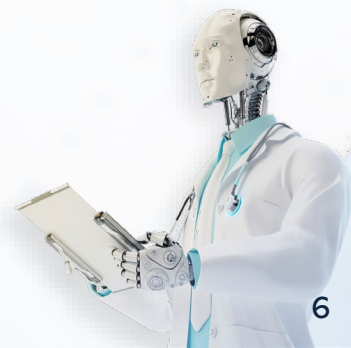
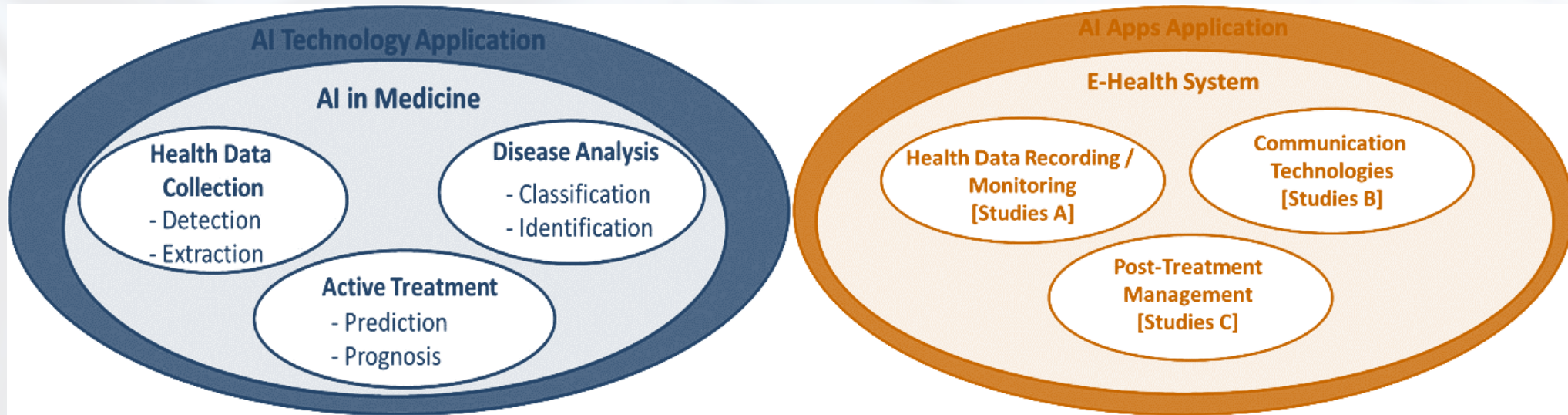
Survey: How long before AI was a noticeable impact on your specialty?



Scheetz, J., Rothschild, P., McGuinness, M. et al. A survey of clinicians on the use of artificial intelligence in ophthalmology, dermatology, radiology and radiation oncology. *Sci Rep* 11, 5193 (2021)



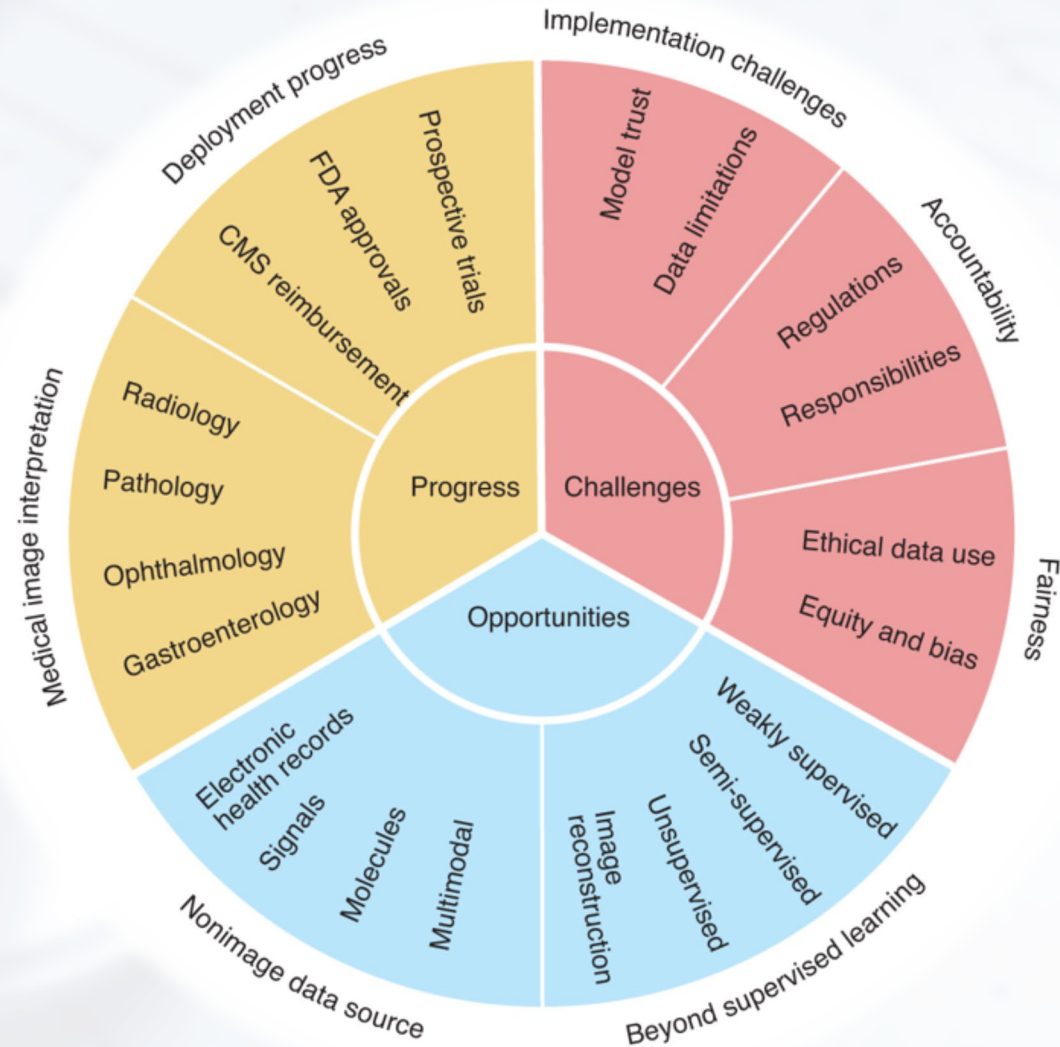
Application of AI in Healthcare areas



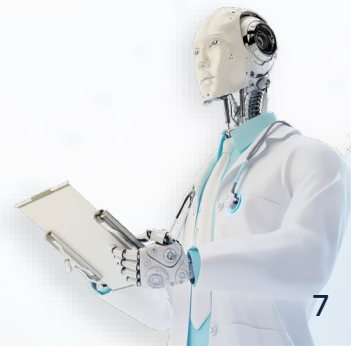
AI in Healthcare



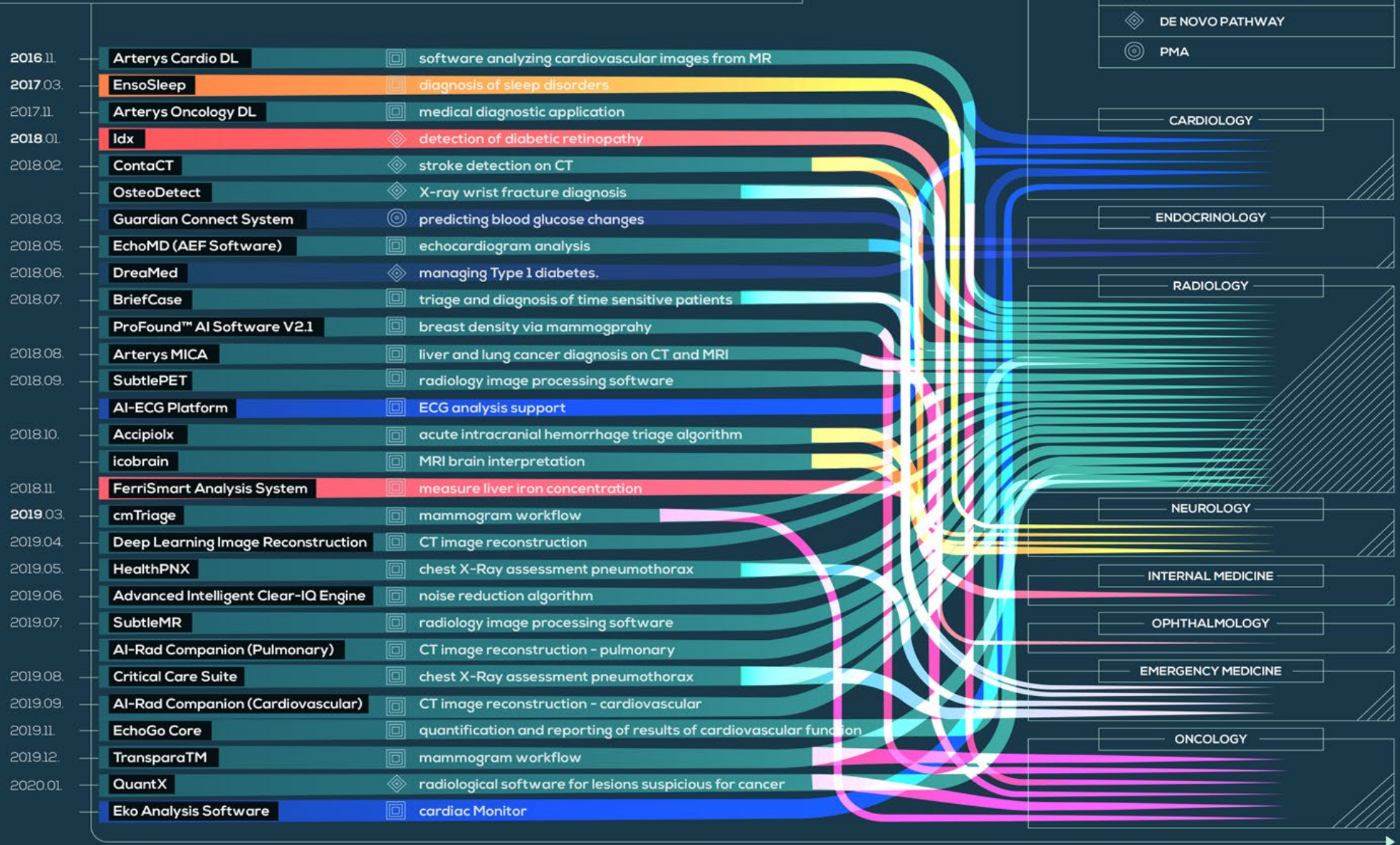
- Progress
- Opportunities
- Challenges



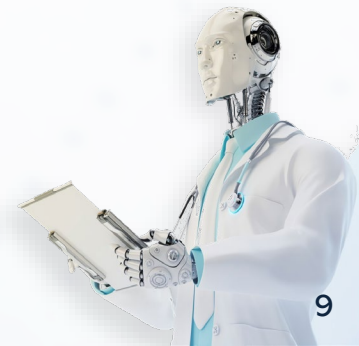
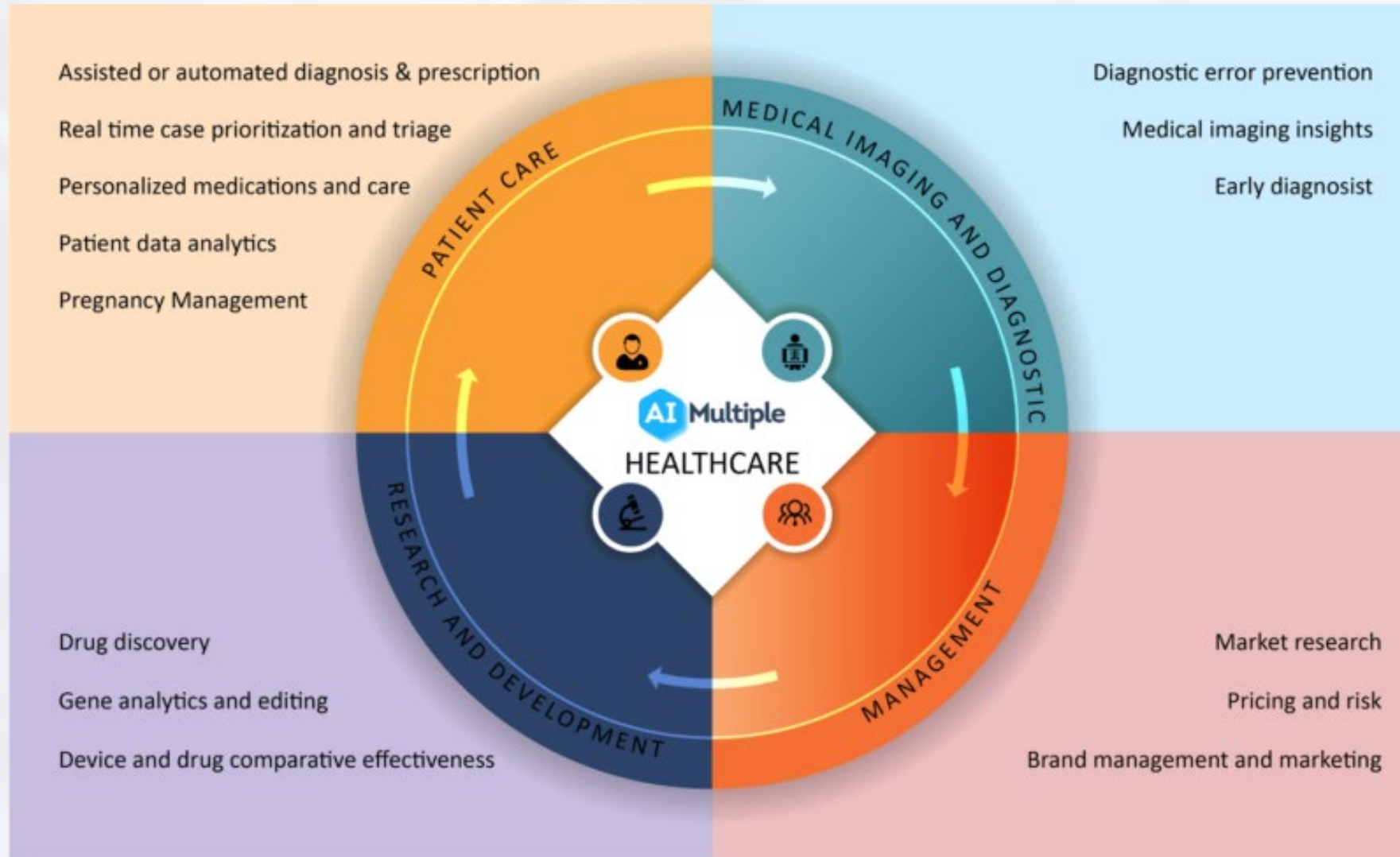
Rajpurkar, P., Chen, E., Banerjee, O. et al. AI in health and medicine. *Nat Med* 28, 31–38 (2022).



FDA APPROVALS FOR ARTIFICIAL INTELLIGENCE-BASED DEVICES IN MEDICINE



Healthcare Use Cases



Healthcare Use Cases



Patient Care

Remote Patient Care



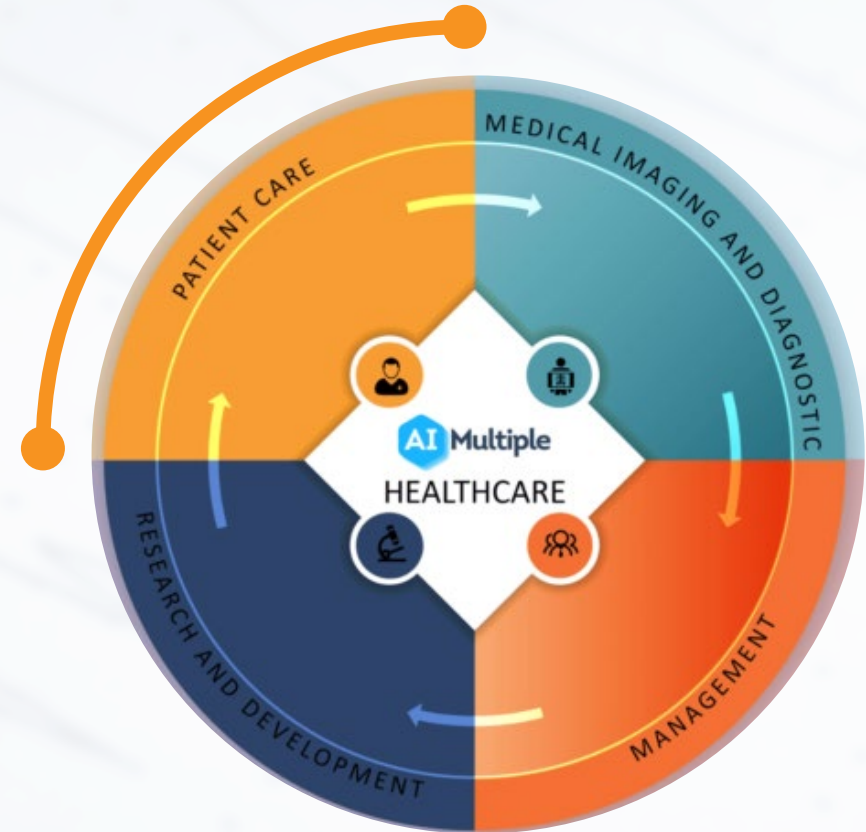
Chatbots can help patients self-diagnose or assist doctors in diagnosis.

Real-time case prioritization and triage.



Personalized medications and care to help users find the best treatment plans according to their patient data.

Surgical robots that allow robot-assisted surgeries combine AI and collaborative robots.



Healthcare Use Cases

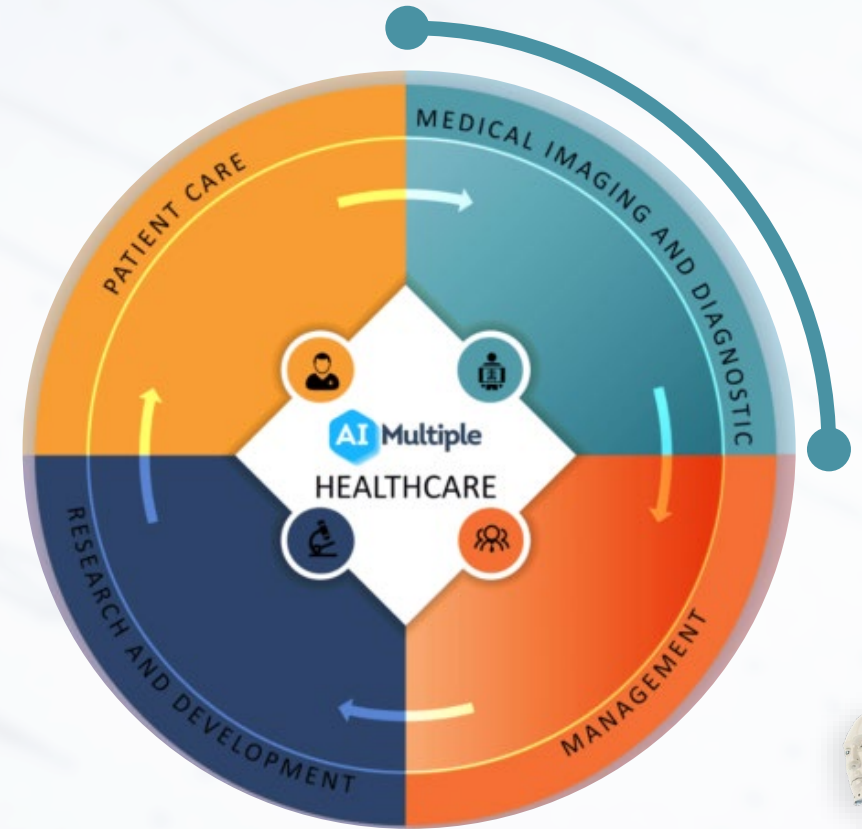


Medical Imaging and Diagnostic



Early diagnosis: Analyze laboratory data and other medical information to facilitate the timely identification of chronic conditions.

Medical imaging insights: Employ advanced medical imaging techniques to analyze images and model potential scenarios.



Healthcare Use Cases



Management



Market analysis: Compile competitive intelligence for hospitals.

Automation technologies, like intelligent automation and RPA, support hospitals in streamlining both routine front-office and back-office tasks, including reporting.



Chatbots for **customer service** enable patients to inquire about matters like bill payment, appointment scheduling, or prescription refills.

Utilizing AI-driven **fraud detection** tools aids hospital administrators in identifying potential fraudulent patients.



Healthcare Use Cases



Research and Development



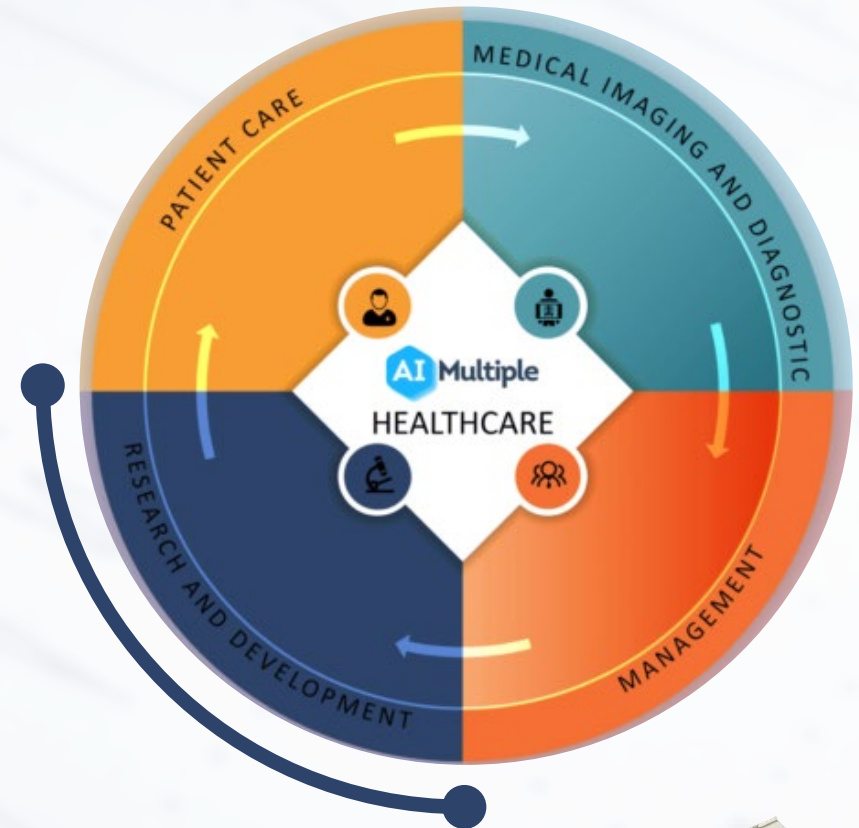
Discover **novel medications** by leveraging historical data and medical insights.

Gene analysis and editing

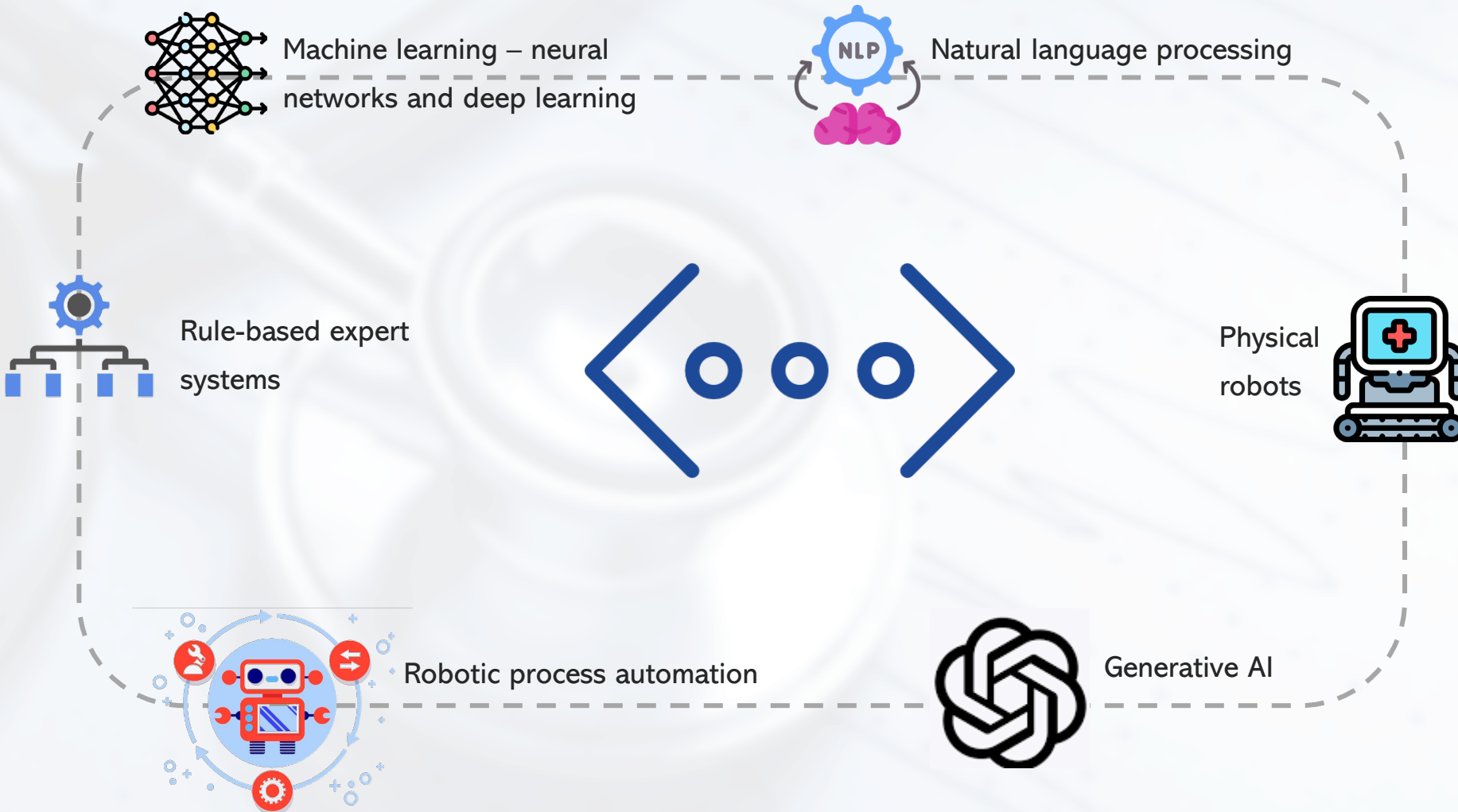


Comparative **effectiveness** of devices and drugs

Pharmaceutical Industry



Technologies



Is AI
secure?

Is it safe to
use AI?

Can we trust
AI?






AI Properties



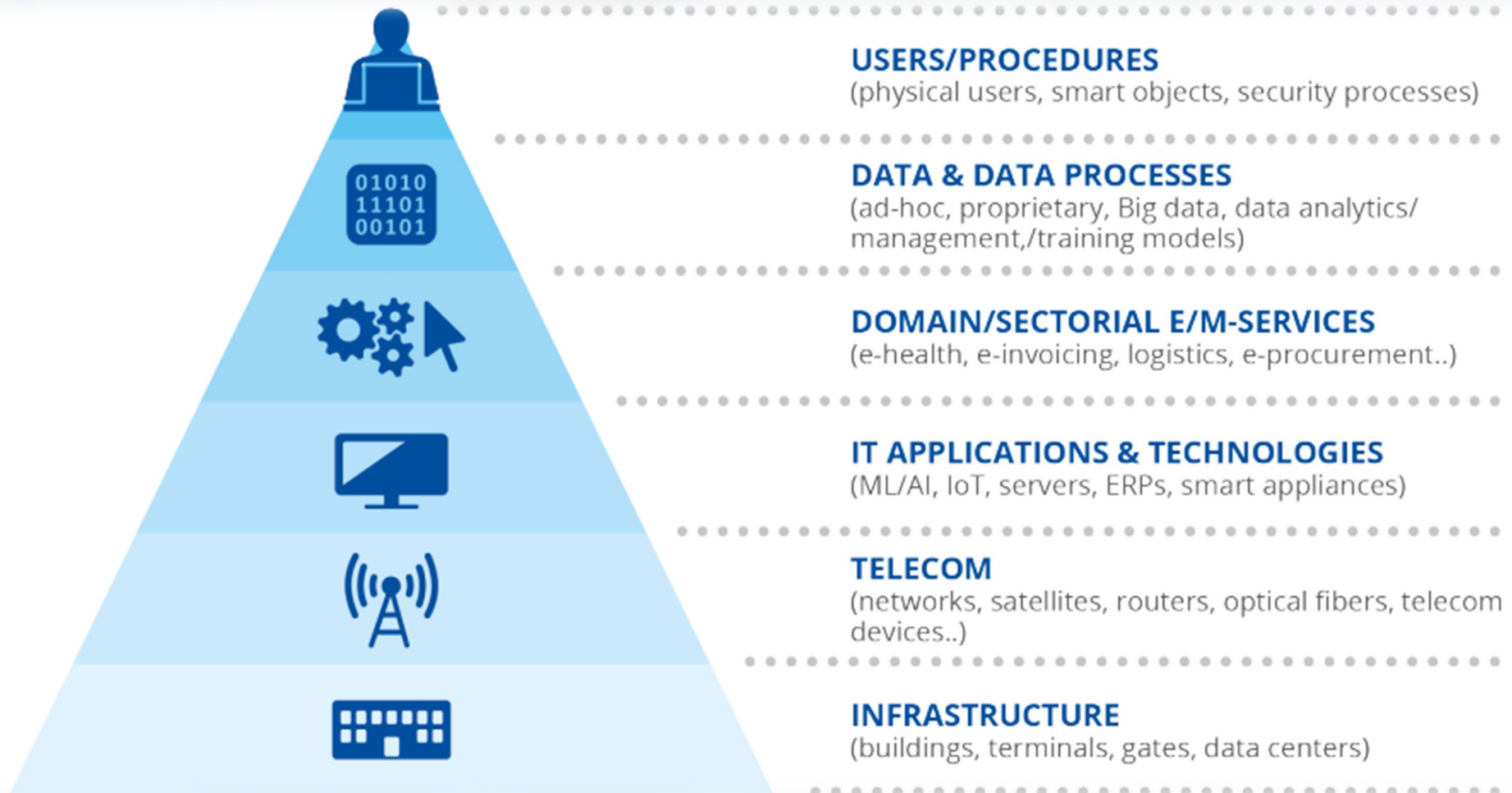
AI characteristics mapping to policy documents



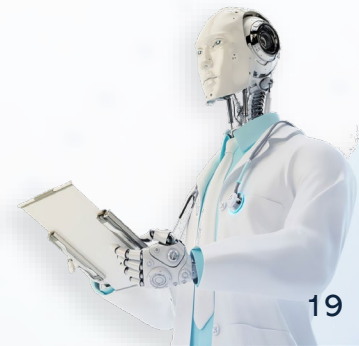
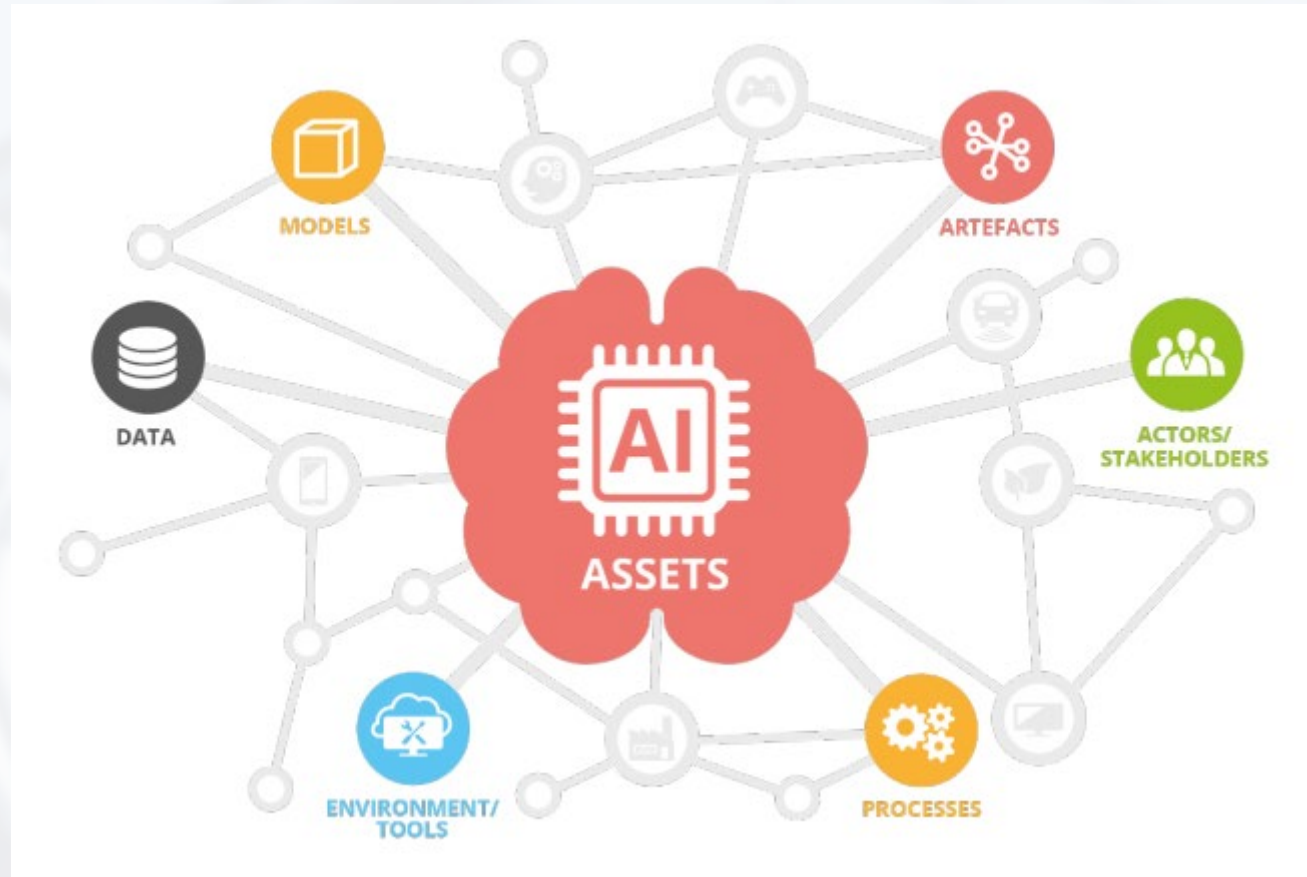
	 TECHNICAL DESIGN CHARACTERISTICS	 SOCIO-TECHNICAL CHARACTERISTICS	 GUIDING PRINCIPLES CONTRIBUTING TO TRUSTWORTHINESS
AI RMF Taxonomy	<ul style="list-style-type: none"> • Accuracy • Reliability • Robustness • Resilience or ML Security 	<ul style="list-style-type: none"> • Explainability • Interpretability • Privacy • Safety • Managing Bias 	<ul style="list-style-type: none"> • Fairness • Accountability • Transparency
OECD AI Recommendation	<ul style="list-style-type: none"> • Robustness • Security 	<ul style="list-style-type: none"> • Safety • Explainability 	<ul style="list-style-type: none"> • Traceability to human values • Transparency and responsible disclosure • Accountability
EU AI Act	<ul style="list-style-type: none"> • Technical Robustness 	<ul style="list-style-type: none"> • Safety • Privacy • Non-discrimination 	<ul style="list-style-type: none"> • Human agency and oversight • Data governance • Transparency • Diversity and fairness • Environmental and societal well-being • Accountability
EO 13960	<ul style="list-style-type: none"> • Purposeful and performance-driven • Accurate, reliable, and effective • Secure and resilient 	<ul style="list-style-type: none"> • Safe • Understandable by subject matter experts, users, and others, as appropriate 	<ul style="list-style-type: none"> • Lawful and respectful of our Nation's values • Responsible and traceable • Regularly monitored • Transparent • Accountable



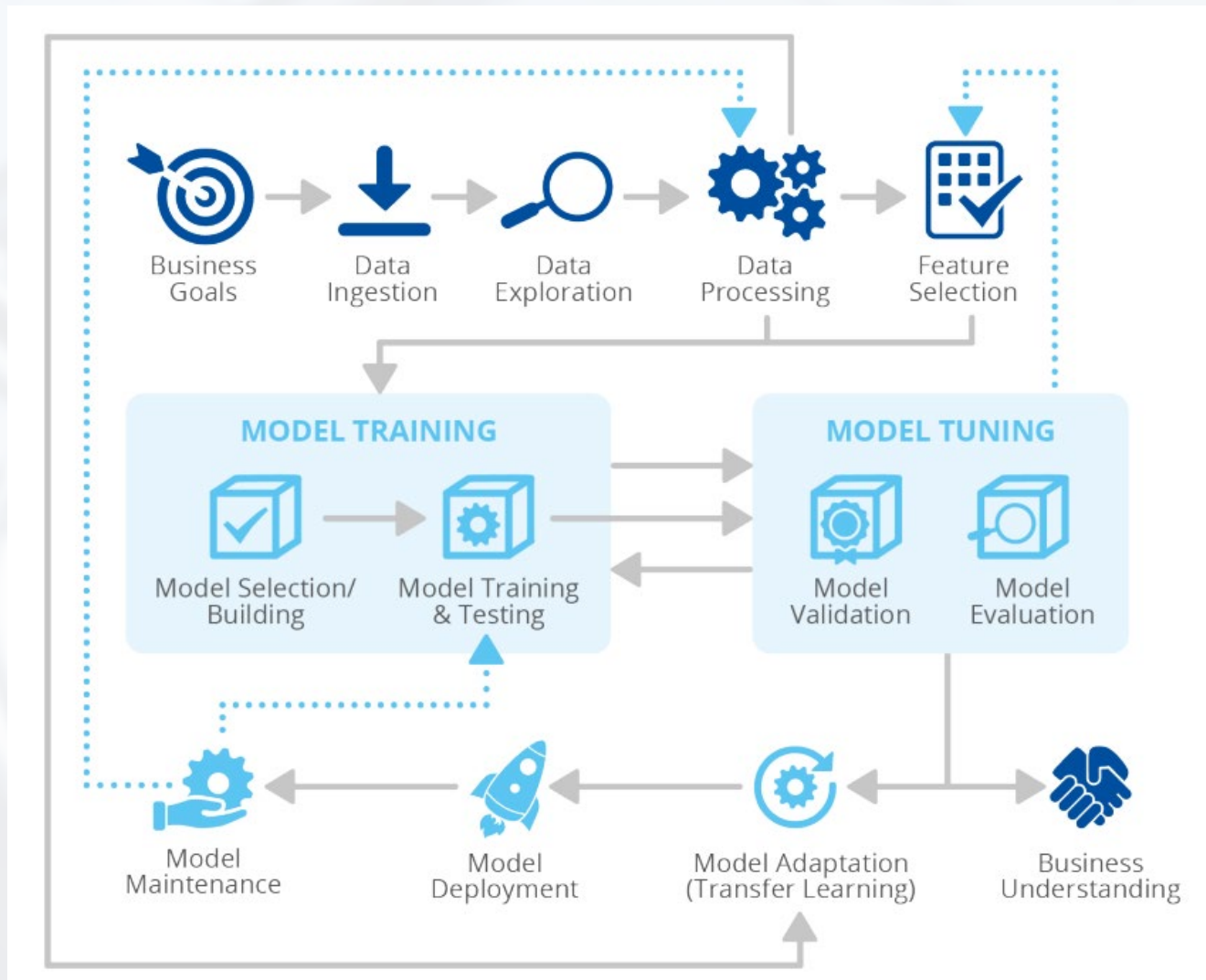
AI security



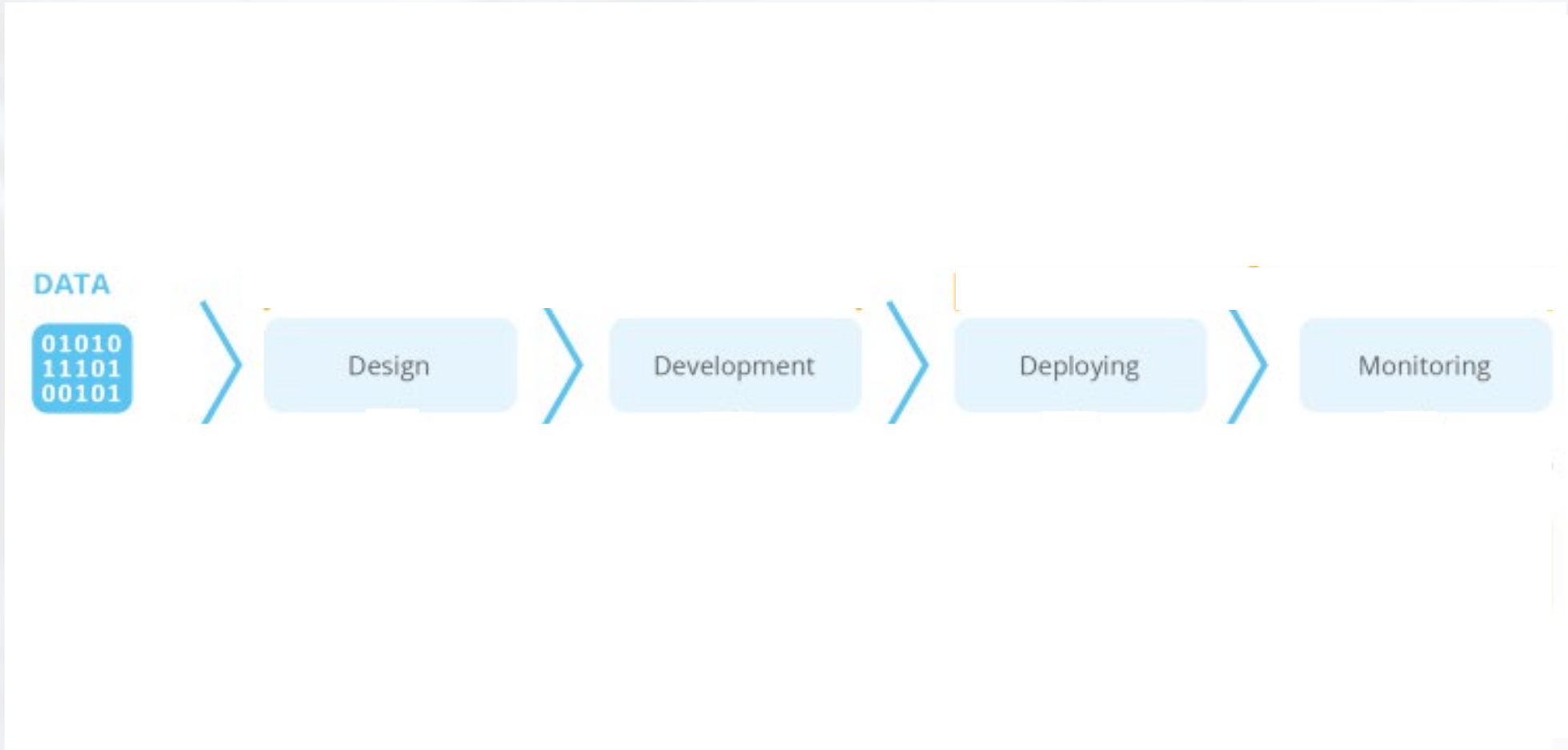
AI Assets



AI lifecycle



AI Challenges



AI Risk Management



Key Dimensions	Application Context	Data & Input	AI Model	AI Model	Task & Output	Application Context	People & Planet
Lifecycle Stage	Plan and Design	Collect and Process Data	Build and Use Model	Verify and Validate	Deploy and Use	Operate and Monitor	Use or Impacted by
TEVV	TEVV includes audit & impact assessment	TEVV includes internal & external validation	TEVV includes model testing	TEVV includes model testing	TEVV includes integration, compliance testing & validation	TEVV includes audit & impact assessment	TEVV includes audit & impact assessment
Activities	Articulate and document the system's concept and objectives, underlying assumptions, and context in light of legal and regulatory requirements and ethical considerations.	Gather, validate, and clean data and document the metadata and characteristics of the dataset, in light of objectives, legal and ethical considerations.	Create or select algorithms; train models.	Verify & validate, calibrate, and interpret model output.	Pilot, check compatibility with legacy systems, verify regulatory compliance, manage organizational change, and evaluate user experience.	Operate the AI system and continuously assess its recommendations and impacts (both intended and unintended) in light of objectives, legal and regulatory requirements, and ethical considerations.	Use system/ technology; monitor & assess impacts; seek mitigation of impacts, advocate for rights.
Representative Actors	System operators; end users; domain experts; AI designers; impact assessors; TEVV experts; product managers; compliance experts; auditors; governance experts; organizational management; C-suite executives; impacted individuals/ communities; evaluators.	Data scientists; data engineers; data providers; domain experts; socio-cultural analysts; human factors experts; TEVV experts.	Modelers; model engineers; data scientists; developers; domain experts; with consultation of socio-cultural analysts familiar with the application context and TEVV experts.	System integrators; developers; systems engineers; software engineers; domain experts; procurement experts; third-party suppliers; C-suite executives; with consultation of human factors experts, socio-cultural analysts, governance experts, TEVV experts,	System operators, end users, and practitioners; domain experts; AI designers; impact assessors; TEVV experts; system funders; product managers; compliance experts; auditors; governance experts; organizational management; impacted individuals/communities; evaluators.	System operators, end users, and practitioners; domain experts; AI designers; impact assessors; TEVV experts; system funders; product managers; compliance experts; auditors; governance experts; organizational management; impacted individuals/communities; evaluators.	End users, operators, and practitioners; impacted individuals/communities; general public; policy makers; standards organizations; trade associations; advocacy groups; environmental groups; civil society organizations; researchers.





MITRE ATLAS™ (Adversarial Threat Landscape for Artificial-Intelligence Systems)

ATLAS™

The ATLAS Matrix below shows the progression of tactics used in attacks as columns from left to right, with ML techniques belonging to each tactic below. & indicates an adaptation from ATT&CK. Click on links to learn more about each item, or view ATLAS tactics and techniques using the links at the top navigation bar.

Reconnaissance & 5 techniques	Resource Development & 7 techniques	Initial Access & 4 techniques	ML Model Access 4 techniques	Execution & 2 techniques	Persistence & 2 techniques	Defense Evasion & 1 technique	Discovery & 3 techniques	Collection & 3 techniques	ML Attack Staging 4 techniques	Exfiltration & 2 techniques	Impact & 7 techniques
Search for Victim's Publicly Available Research Materials	Acquire Public ML Artifacts	ML Supply Chain Compromise	ML Model Inference API Access	User Execution &	Poison Training Data	Evade ML Model	Discover ML Model Ontology	ML Artifact Collection	Create Proxy ML Model	Exfiltration via ML Inference API	Evade ML Model
Search for Publicly Available Adversarial Vulnerability Analysis	Obtain Capabilities &	Valid Accounts &	ML-Enabled Product or Service	Command and Scripting Interpreter &	Backdoor ML Model		Discover ML Model Family	Data from Information Repositories &	Backdoor ML Model	Exfiltration via Cyber Means	Denial of ML Service
Search Victim-Owned Websites	Develop Adversarial ML Attack Capabilities	Evade ML Model	Physical Environment Access				Discover ML Artifacts	Data from Local System &	Verify Attack		Spamming ML System with Chaff Data
Search Application Repositories	Acquire Infrastructure	Exploit Public-Facing Application &	Full ML Model Access						Craft Adversarial Data		Erode ML Model Integrity
Active Scanning &	Publish Poisoned Datasets										Cost Harvesting
	Poison Training Data										ML Intellectual Property Theft
	Establish Accounts &										System Misuse for External Effect

Thank You!

Isabel Praça

icp@isep.ipp.pt

