Accelerate Human-Machine Teaming

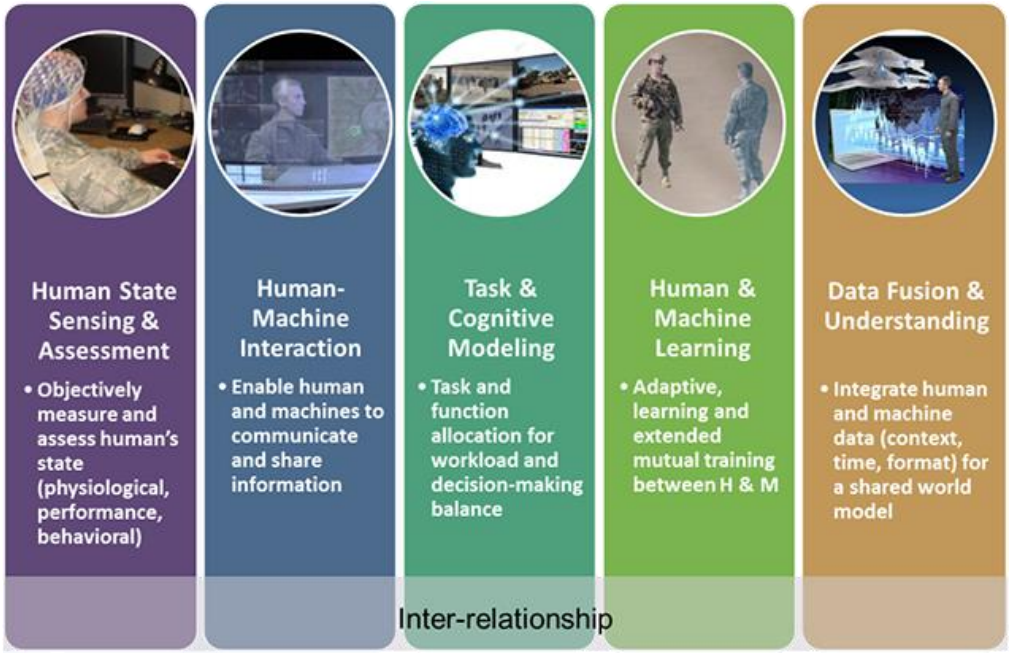
Empowering the Workforce to embrace the AI future

Bill Nystrom
Chief Technology Officer
Secure Networks

Telos®

DAFITC 2022

Human Machine Teaming Vision



Published by AFRL in 2014

Competition breeds excellence

china population compared to us

ALL WORK IMAGES VIDEOS MAPS NEWS SHOPPING MORE

8,090 Results

4.35 times the US population

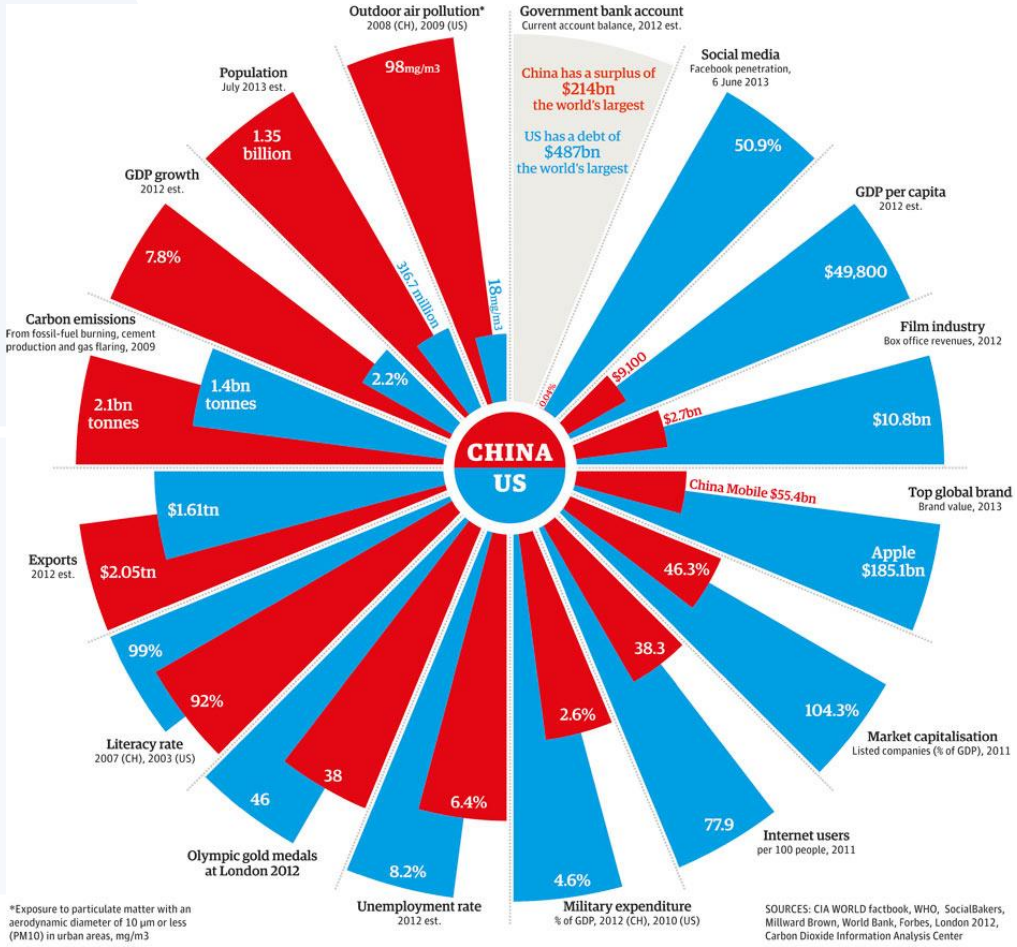
China population is **4.35 times the US population**, with China home to about 1.44 billion people and the United States to 331 million in 2020. The population of China will peak in 2031, but the US will not peak until 2100. China is four times denser than the US as China's population density is 153 people per square km compared to 36 of the US.

Date: 10 Jan 2021

Source: UN (World Population Prospects 2019)

United States vs China by population - StatisticsTimes.com
statisticstimes.com/demographics/china-vs-us-population.php

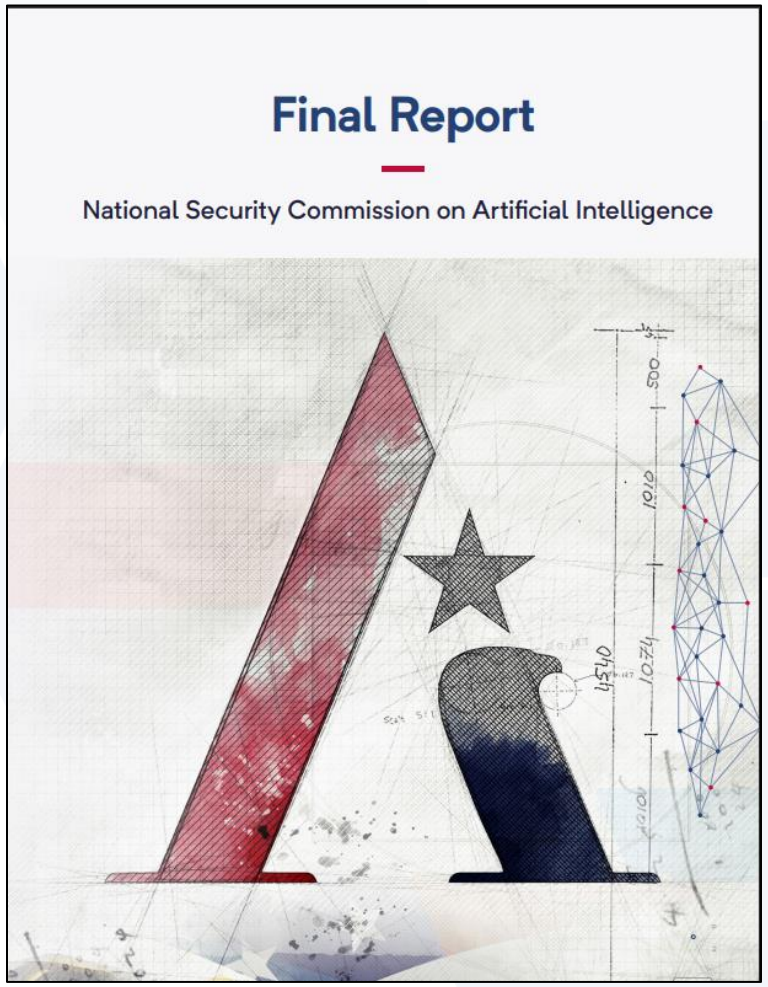
Was this helpful?



Telos®

National Call to Action

By 2025, the foundations for widespread integration of AI across the Department of Defense must be in place.



Foundations of Future Defense

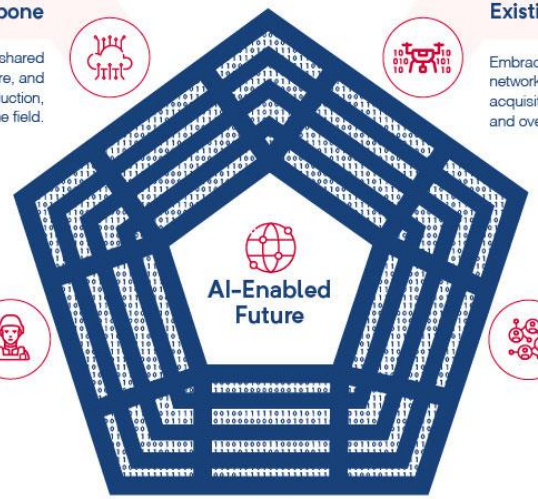
Necessary actions to create a defense department that is ready to leverage AI at speed and scale.

Build the Technical Backbone

Provide a common platform of shared services–including data, software, and compute–that support development, production, and integration from the laboratory to the field.

Accelerate Adoption of Existing Digital Technologies

Embrace commercial AI applications, network digital innovation initiatives, optimize acquisition, and establish more agile budget and oversight mechanisms.



Train and Educate Warfighters

Establish ability to integrate, interact with, and experiment with AI as core competencies across the force.

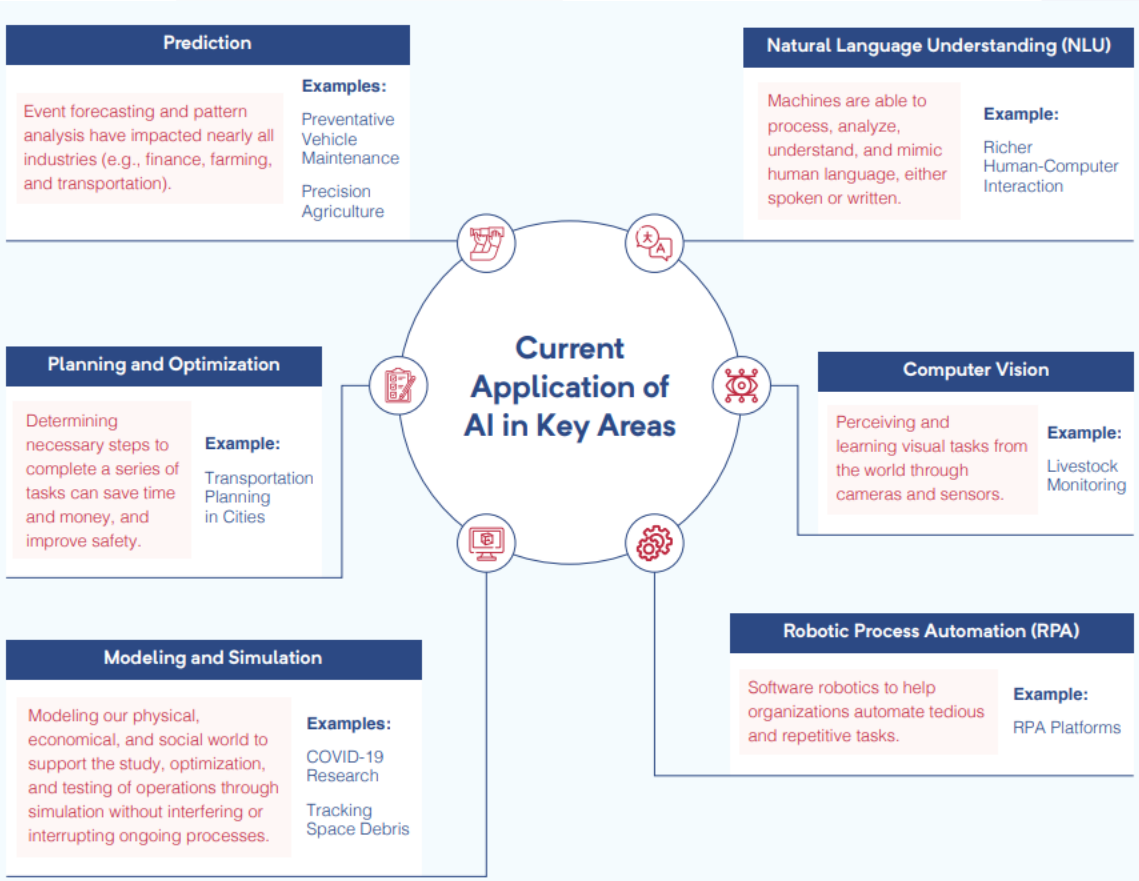
Democratize Development

Democratize development through enterprise platforms, JAIC's role as the AI accelerator, AI delivery teams at every Combatant Command, and forward-deployed developers.

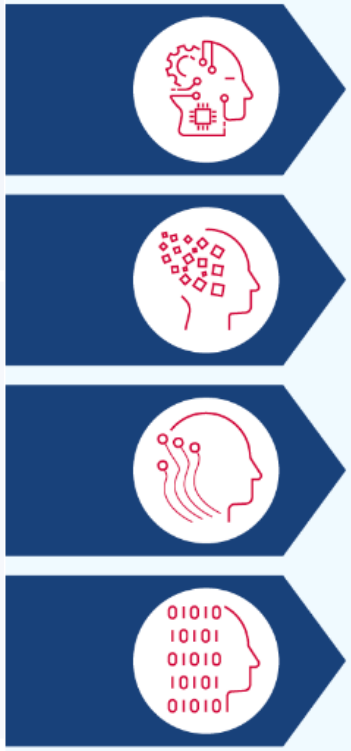
Invest in Next-Generation Capabilities

Divest from legacy systems, identify critical technologies and applications, and increase S&T funding to drive progress in those areas.

NSCAI AI Landscape



To achieve dominance in AI, the U.S. needs to train four archetypes to propel AI in America: researchers, implementers, end users, and informed consumers.



Researchers

AI research engineers will focus on R&D of technologies that enable and advance semi- and fully-autonomous systems. They serve as algorithm experts with up-to-date knowledge of modern AI research and may be involved in the inception of ideas and drive the development cycles from research to testing of prototypes for a major project or component of a major project.

Implementers

They will be responsible for data cleaning, feature extraction and selection, and analysis; model training and tuning; partnerships with domain knowledge experts and end users; and the discovery of local opportunities for exploitation. Developers require less training and education than AI experts, and will have training, education, and/or experience that is roughly equivalent to an associate or bachelor's degree; and that includes relevant ethics and bias mitigation in data processing and model training.

End Users

They will have their daily business augmented/enabled by AI. Use of AI will strongly resemble the use of currently available software in that it will require some system-specific training, but, with the exception of some positions that manage data, little to no AI specific expertise.

Informed Consumers

This group of people needs the ability to make better consumer choices when purchasing technology and understand the importance of their actions in the market.

Pervasive AI is a Talent and Training Issue

Talent

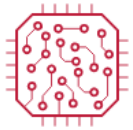
We regard talent as the most essential requirement because it drives the creation and management of all the other elements.

Data

Data is critical for most AI systems.[3] Labeled and curated data enables much of current machine learning (ML) used to create new applications and improve the performance of existing AI applications.

Hardware

The underlying hardware provides the computing power to analyze ever-growing data pools and run applications. This hardware layer includes cloud-based compute and storage, supported by a networking and communications backbone, instrumental for connecting smart sensors and devices at the network edge.



Algorithims

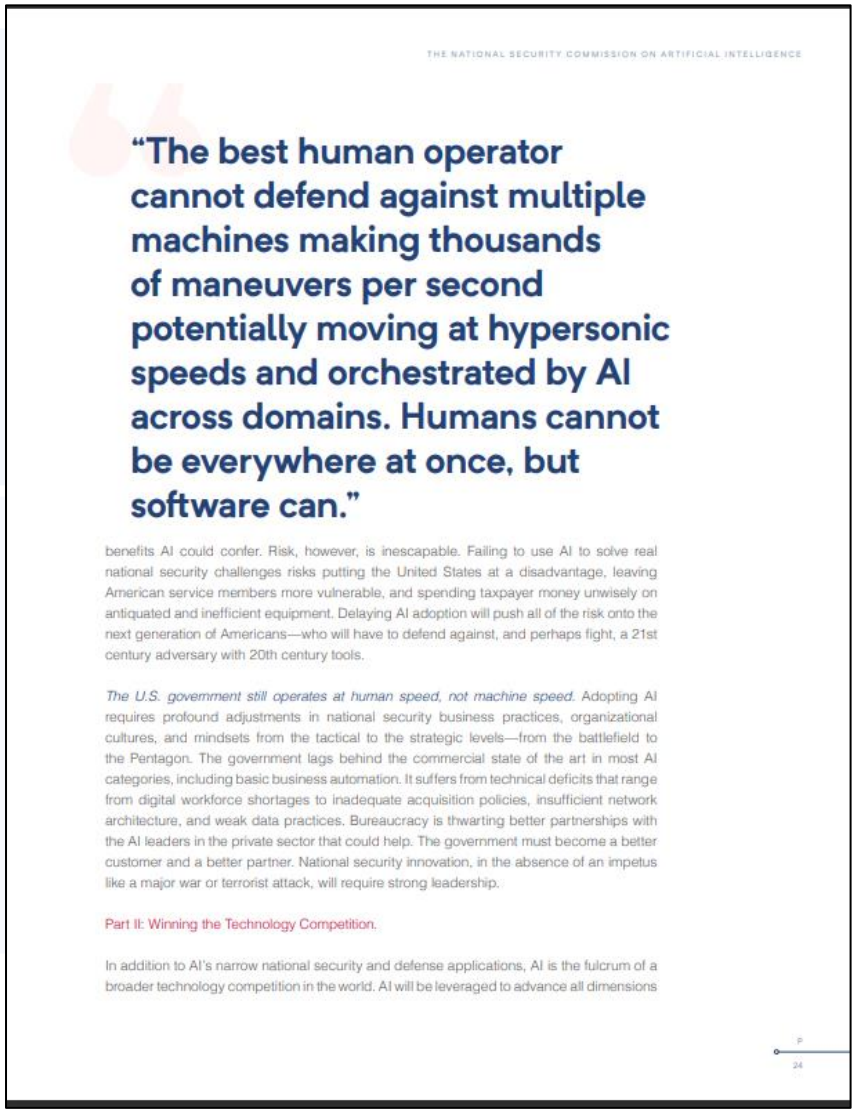
Algorithms are the mathematical operations that tell the system how to navigate the data to provide answers in response to specifi c questions.

Applications

An application makes the answers useful for specific tasks.

Integration

Integration of these elements is critical to fi elding a successful end-to-end AI system. This requires signifi cant engineering talent and investment to integrate existing data fl ows, decision pipelines, legacy equipment, testing designs, etc. This task of integration can be daunting and historically has been underestimated.[4]



THE NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE

"The best human operator cannot defend against multiple machines making thousands of maneuvers per second potentially moving at hypersonic speeds and orchestrated by AI across domains. Humans cannot be everywhere at once, but software can."

benefits AI could confer. Risk, however, is inescapable. Failing to use AI to solve real national security challenges risks putting the United States at a disadvantage, leaving American service members more vulnerable, and spending taxpayer money unwisely on antiquated and inefficient equipment. Delaying AI adoption will push all of the risk onto the next generation of Americans—who will have to defend against, and perhaps fight, a 21st century adversary with 20th century tools.

The U.S. government still operates at human speed, not machine speed. Adopting AI requires profound adjustments in national security business practices, organizational cultures, and mindsets from the tactical to the strategic levels—from the battlefield to the Pentagon. The government lags behind the commercial state of the art in most AI categories, including basic business automation. It suffers from technical deficits that range from digital workforce shortages to inadequate acquisition policies, insufficient network architecture, and weak data practices. Bureaucracy is thwarting better partnerships with the AI leaders in the private sector that could help. The government must become a better customer and a better partner. National security innovation, in the absence of an impetus like a major war or terrorist attack, will require strong leadership.

Part II: Winning the Technology Competition.

In addition to AI's narrow national security and defense applications, AI is the fulcrum of a broader technology competition in the world. AI will be leveraged to advance all dimensions

Democratizing Human-Machine Competency

At the core of future military advantage will be the effective integration of humans, artificial intelligence (AI) and robotics into warfighting systems – human-machine teams – that exploit the capabilities of people and technologies to outperform our opponents.

The game of chess provides an excellent example of human-computer collaboration and a cautionary tale about over-extrapolating when computers outperform humans. In 1997, IBM's Deep Blue beat the chess grandmaster Garry Kasparov. Many observers regarded this, and the subsequent triumph of DeepMind's artificial intelligence (AI) at the game of Go, along with AI that consistently beats Top Gun instructors in air-to-air combat, as the beginning of the end for human cognitive dominance.

However, evidence suggests that the future is more complex than machine beats human. A useful example comes from chess in 2005; a competition was held allowing any combination of human and computer chess players to compete. The competition resulted in an unexpected victory that Kasparov later reflected on:

The Hidden Power of HMT

The surprise came at the conclusion of the event.
The winner was revealed to be not a grandmaster with a state-of-the-art PC but a **pair of amateur American chess players using three computers at the same time.**

Their skill at manipulating and ‘coaching’ their computers to look very deeply into positions effectively counteracted the superior chess understanding of their grandmaster opponents and the greater computational power of other participants.

Weak human + machine + better process was superior to a strong computer alone and, more remarkably, superior to a strong human + machine + inferior process…

Human strategic guidance combined with the tactical acuity of a computer was overwhelming.

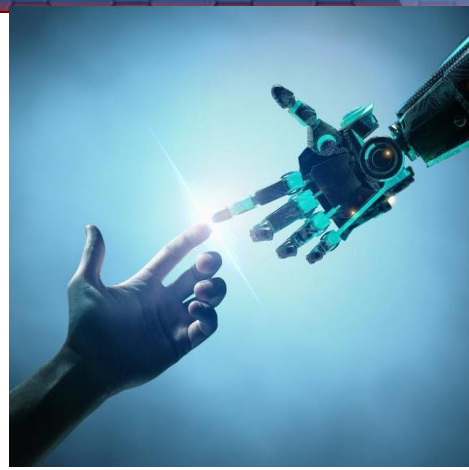
AI is changing relationships between humans and machines

In modern society, we already rely much more on machines and automation than we may be aware. The U.S. military, for instance, has used autonomous systems for decades. However, as AI capabilities improve, the **dynamics within human-machine "teams" will change.** In the past, computers could only perform tasks that fell within a clearly defined set of parameters or rules programmed by a human.

As AI becomes more capable, computers will be able to learn and perform tasks based on parameters that humans do not explicitly program, creating choices and taking actions at a volume and speed never before possible.

Across many fields of human activity, AI innovations are raising important questions about **what choices to delegate to intelligent machines, in what circumstances, and for what reasons.** In the national security sphere, these questions will take on greater significance as AI is integrated into defense and intelligence systems. Across our entire society, we will need to address these new complexities with nuanced approaches, intellectual curiosity, and care that recognizes the increasing ubiquity of AI.

Why Human Machine Teaming



Optimizing human-machine teaming. Optimizing human-machine teaming requires an **understanding of what humans are best at and what machines are best at in the era of narrow AI.**

The last roles likely to be automated will be where personnel conduct activities that demand contextual assessment and agile versatility in complex, cluttered and congested operating areas. **Optimizing how we use human mental and physical capacity within such a force will become a key factor in out-maneuvering and out-thinking opponents.**

High quality live and synthetic collective training and experimentation will be vital for humans to understand the strengths, weaknesses and critical limitations of such AI systems while also providing vital data to improve AI responses, including about human behaviors in the team

Trust and assurance for artificial intelligence.

The increasing array of capabilities of robotic and AI systems will be limited by not only what can be done, but also by what actors trust their machines to do.

The more capable our AI systems are, the greater their ability to conduct local processing and respond to more abstract, higher level commands. **The more we trust the AI, the lower the level of digital connectivity we will demand to maintain system control.**

Developing appropriate standards and robust assurance and certification regimes will be critical, along with effective mechanisms to demonstrate meaningful human accountability.

Although legal obligations and policies are unlikely to cede an opponent military advantage in the near term, as future technologies emerge, particularly for systems supporting targeting and fires, we must consider the ethical and legal implications.

Accessing skills and the race for technological advantage.

The major strategic issue for all actors – nations or technology giants – is a chronic skills shortage.

There is a significant shortage of skilled graduates, software engineers and computer technology staff with the necessary skills to develop the full breadth of possible AI-enabled technologies.

Early investment in education to generate subject matter expertise may represent the critical long term source of economic and military advantage for a nation. For some technologies, such as lethal effects or stealth, only the military will lead primary investment and must continue to do so for disruptive advantage. However, investment and development in the commercial sector will exceed Government research investment for other applications.

The ability to exploit commercial technology developments in Defense-industrial partnerships faster

Trust is already hard

THE TRUST EQUATION

$$\text{TRUST} = \frac{\text{CREDIBILITY} + \text{RELIABILITY} + \text{INTIMACY}}{\text{SELF-ORIENTATION}}$$

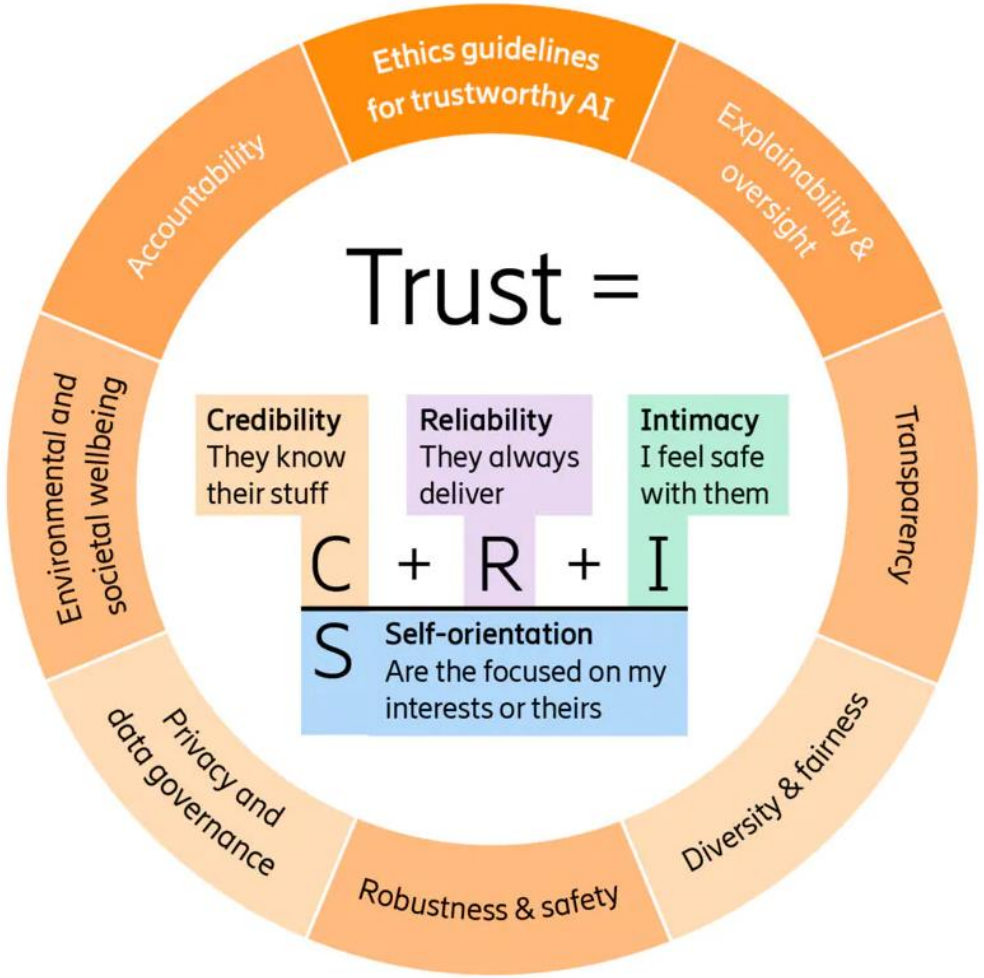
Credibility (Words) – *I can trust what he says about…*

Reliability (Actions) – *I can trust her to…*

Intimacy (Emotions) – *I feel comfortable discussing this…*

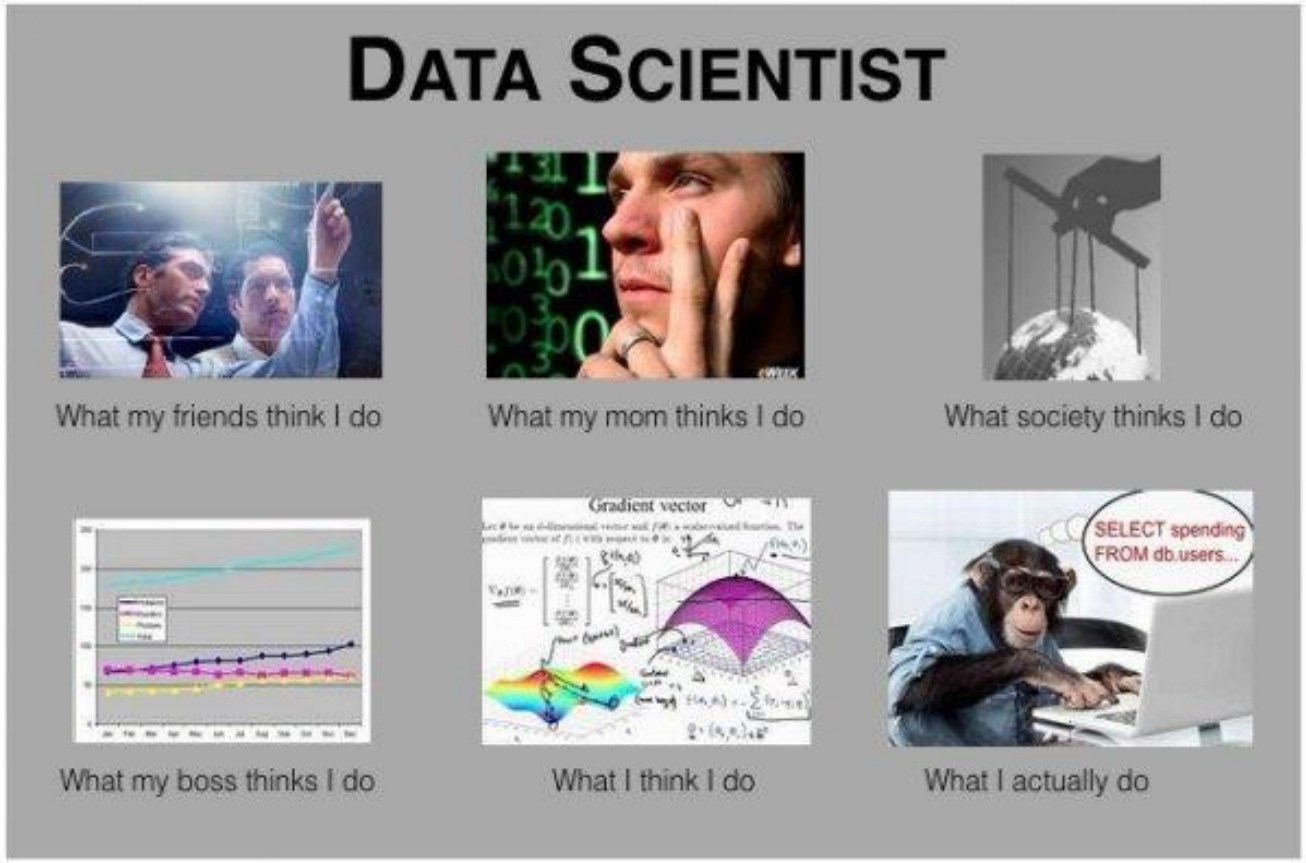
Self-orientation (Motives) – *Who does the advisor care about?*

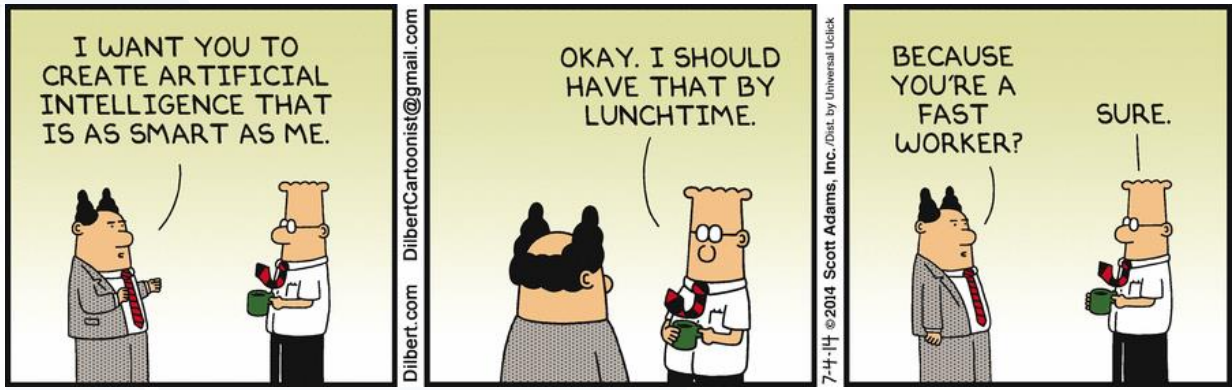
Trust is even harder when we add AI



Workforce views AI with caution

AI is someone else's job

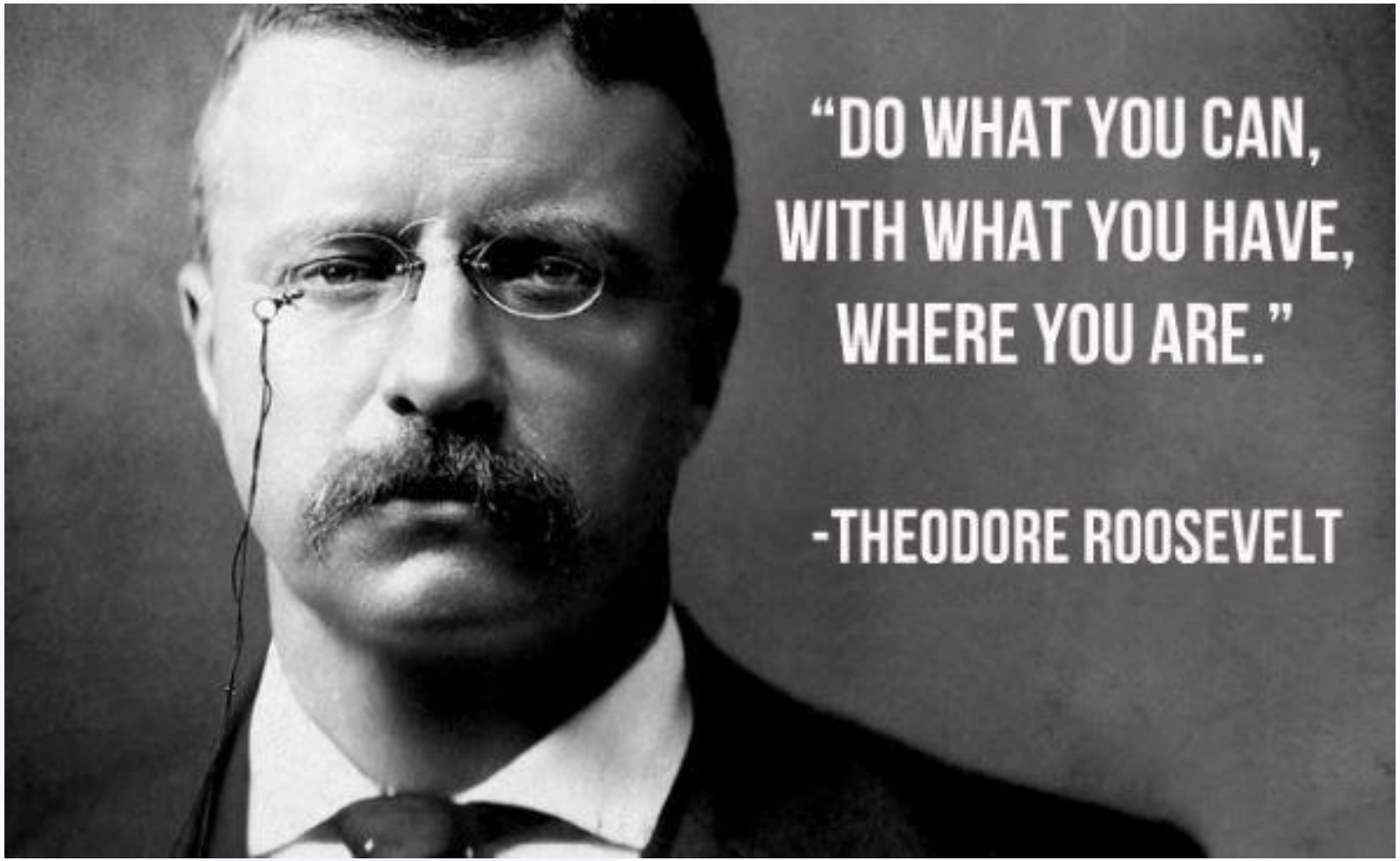




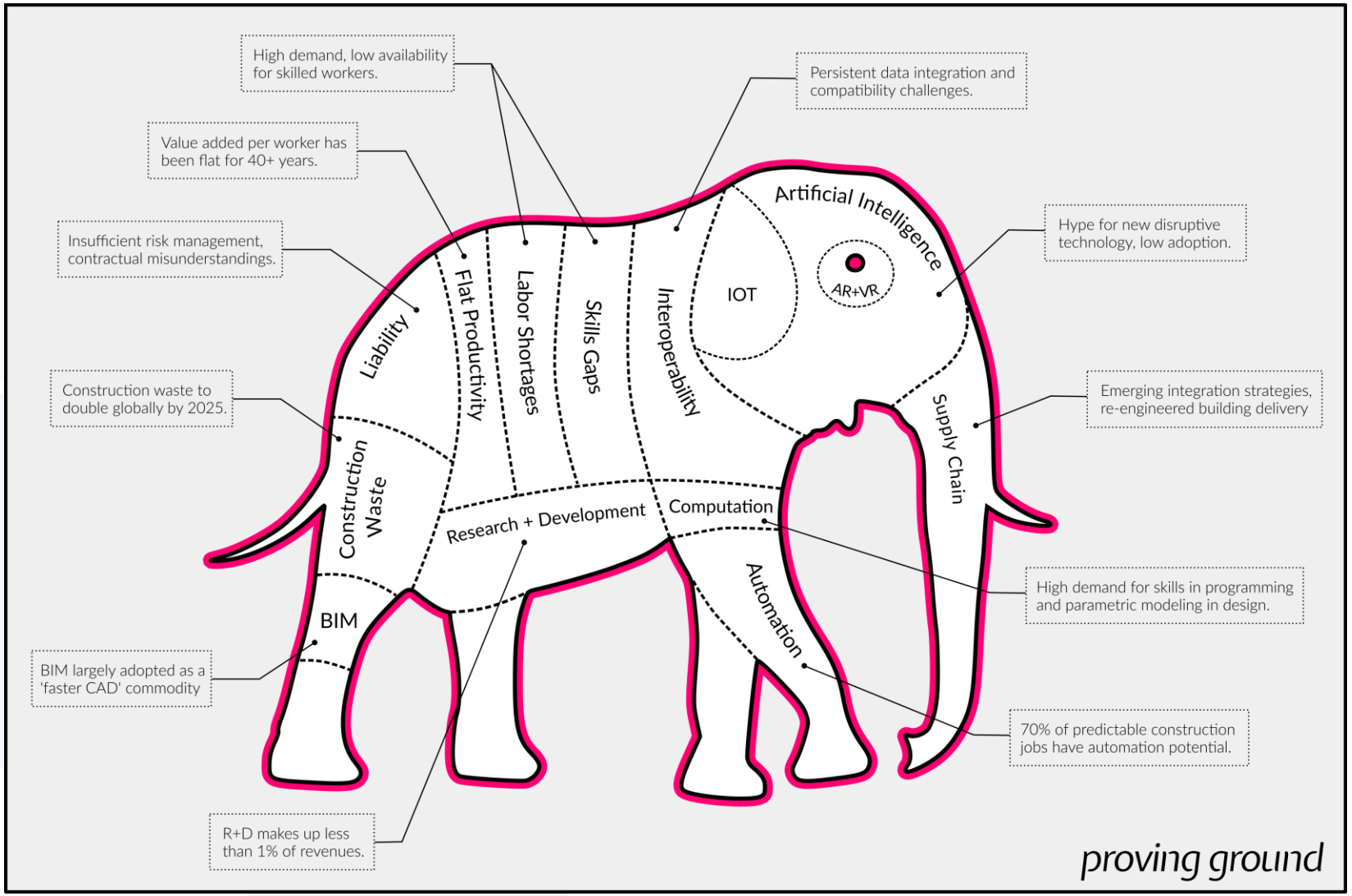
AI is may take my job

Both perspectives are ineffective to advancing AI capabilities

It is time to start building a relationship



How do you eat an elephant?

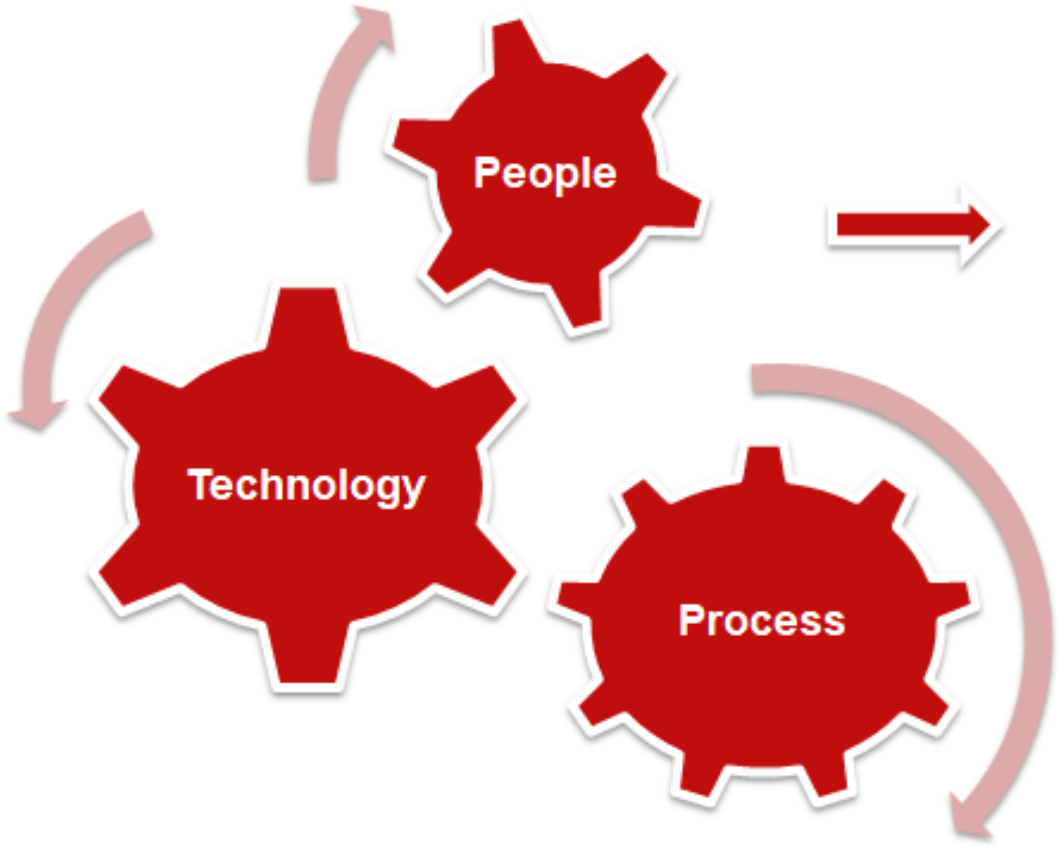


Hard Truth

AI is not possible without Automation

Leverage Enterprise RPA to build AI skills

Friction between People, Process, and Technology facets



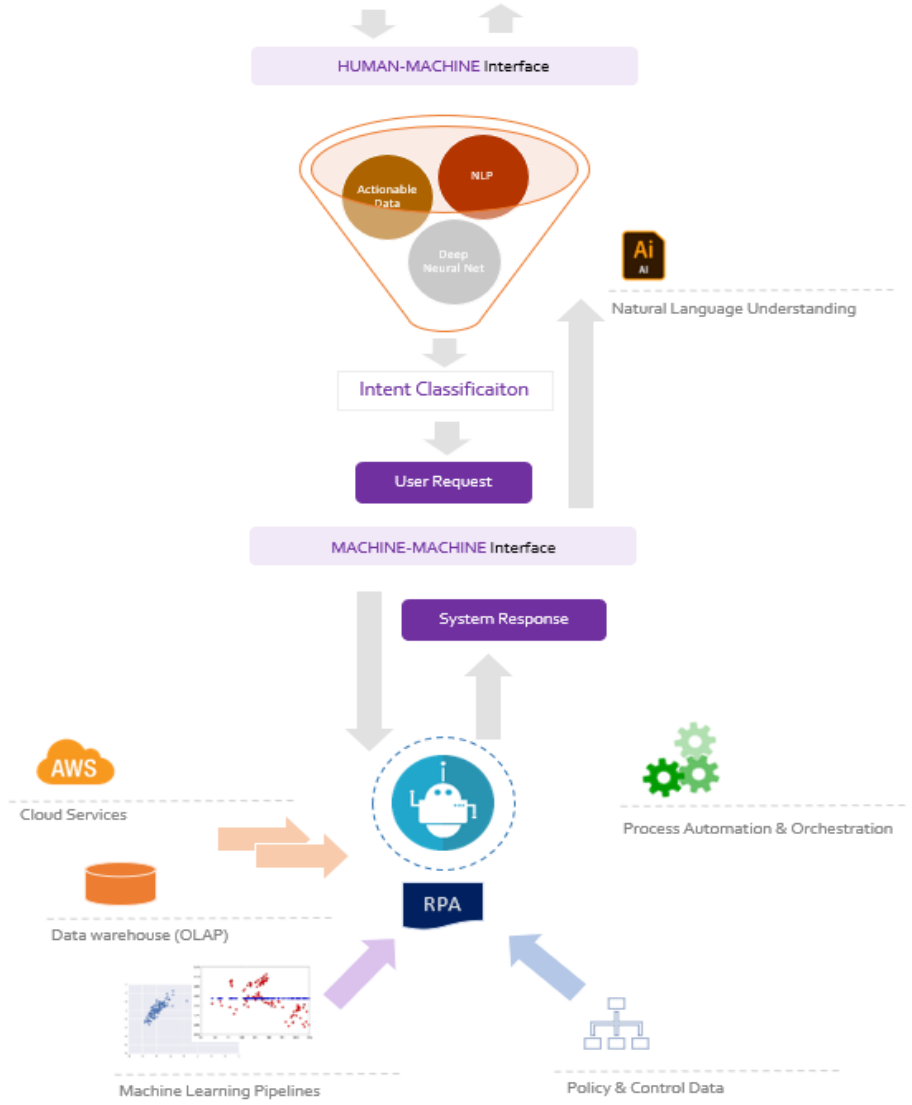
RPA scalability & implementation challenges

- Fragmented processes
- No end-to-end process automation
- No monitoring capability

- Skills shortage, business users left behind
- Poor change management
- Lack of ownership

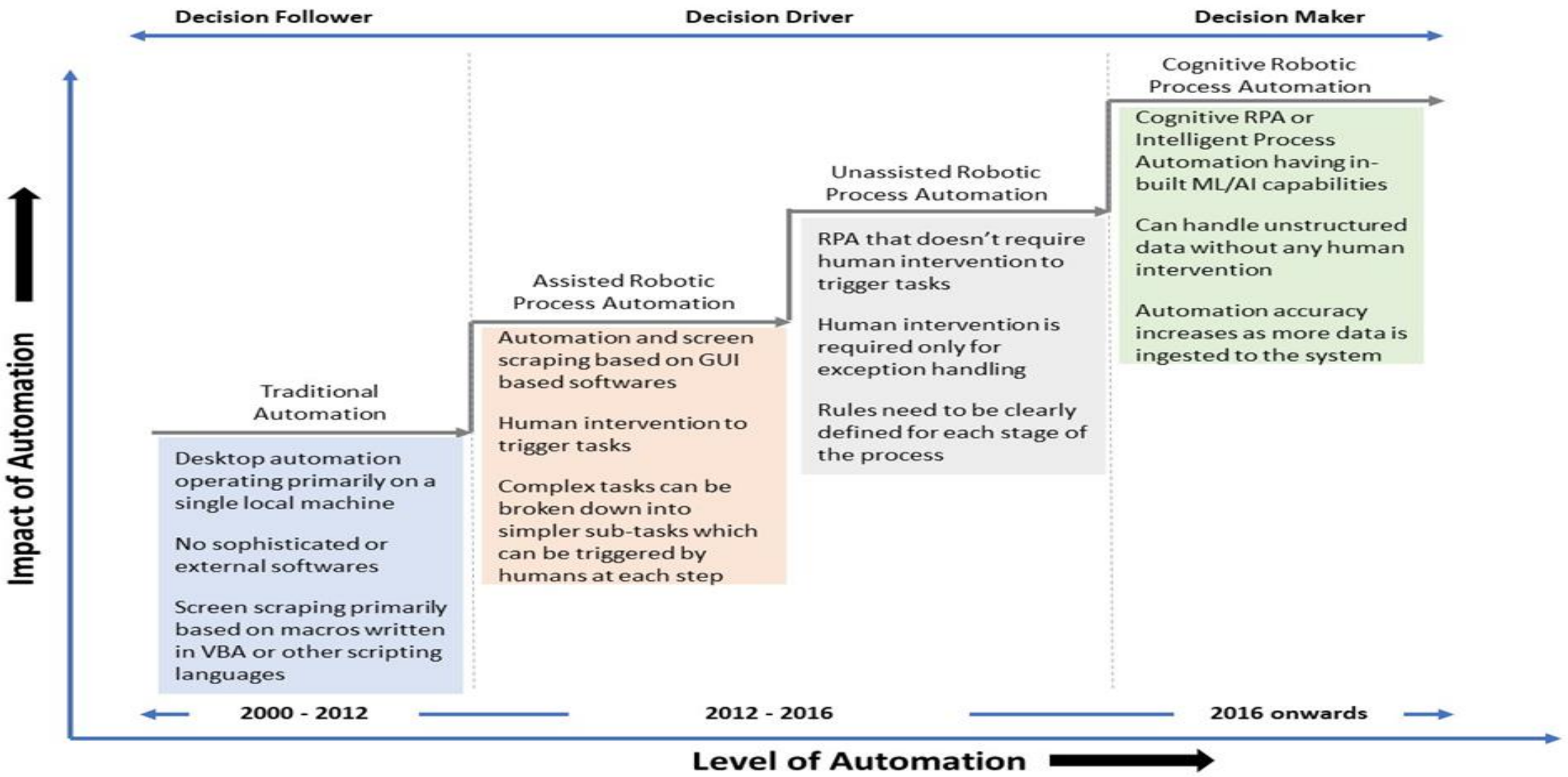
- Lack of IT involvement
- Disregard for infrastructure management
- Lack of governance and stewardship

Automation Practical Flow – Pre ML

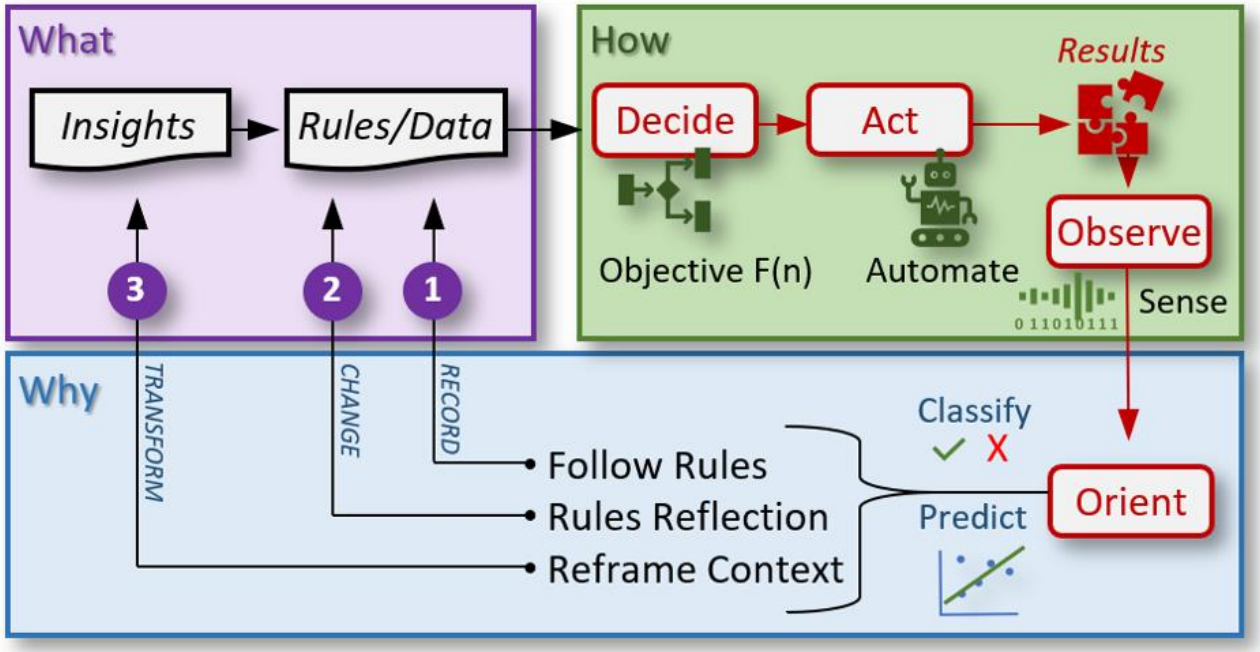


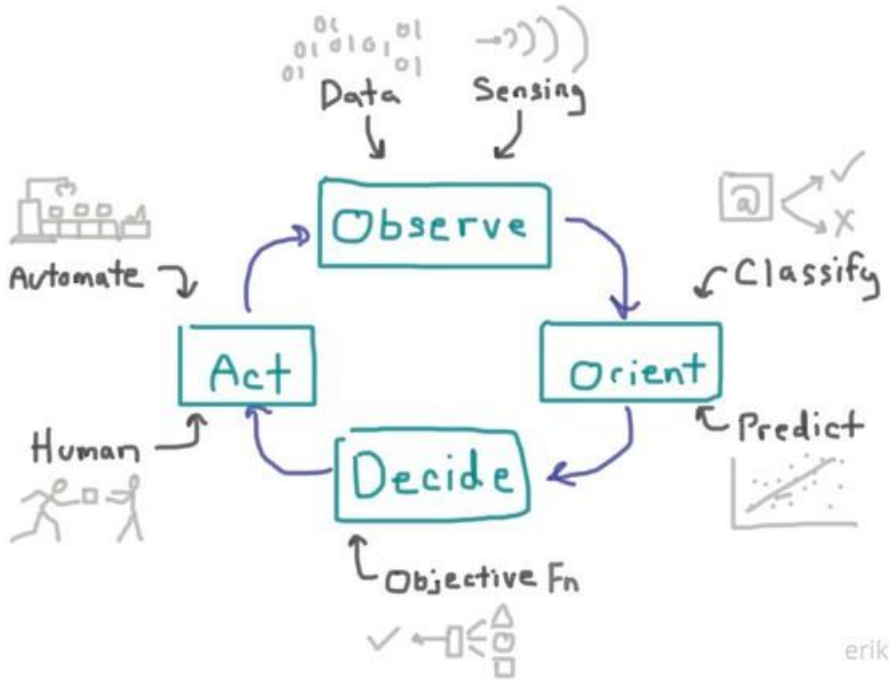
RPA	NLP	Deep Learning
• Action triggers • HTTP/REST • Application hooks via API • Orchestrators	• Text Stemming, Lemmatization • CRF (text classification) • Pattern recognition	• LSTM • RNN
UI Path, Blue Prism, Ansible/Chef	SpaCy, NLTK, Rasa nlu	Python, Scikit-learn, Keras

Automation Maturity – Path to AI

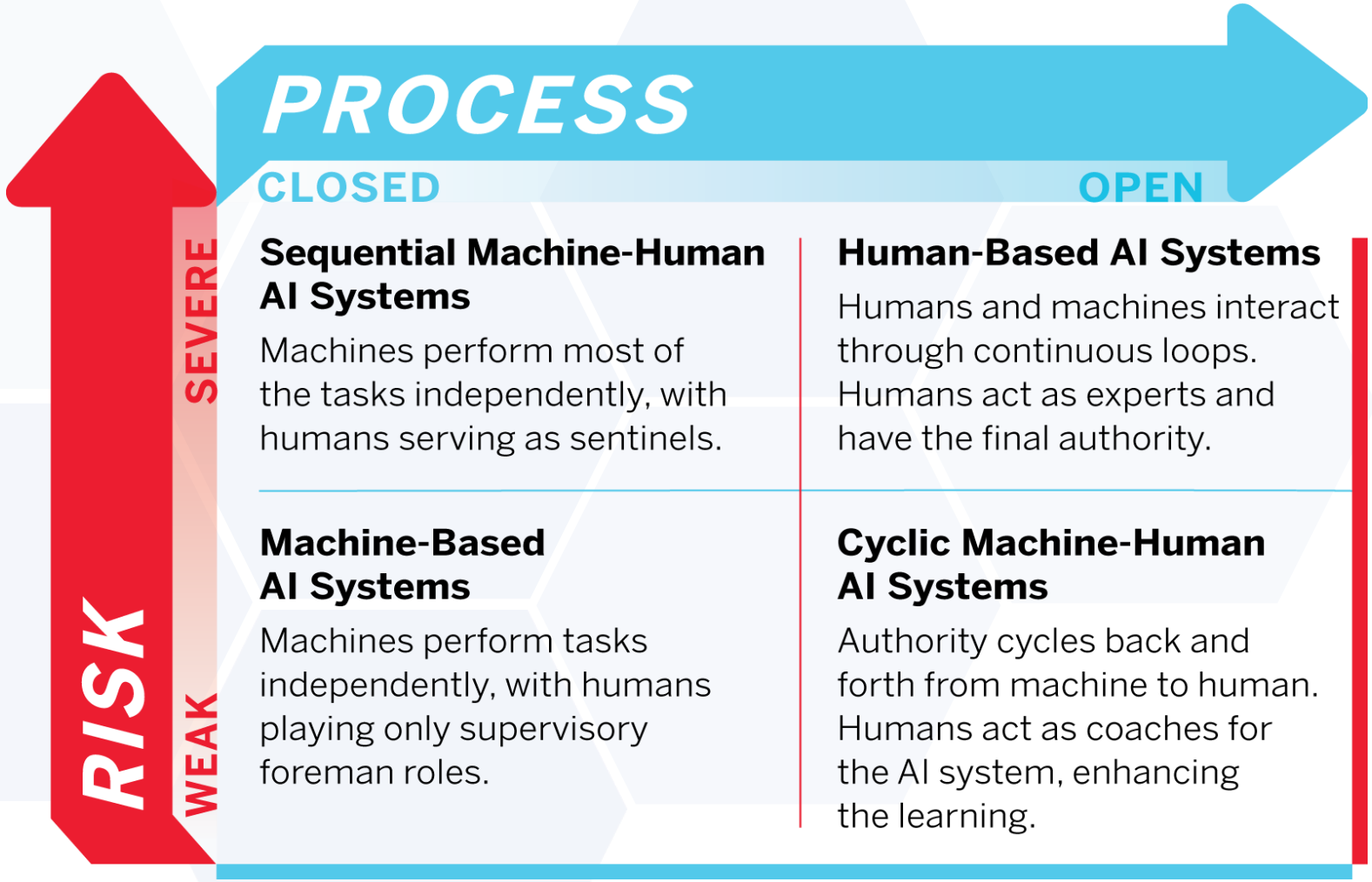


Automation framework to decision AI

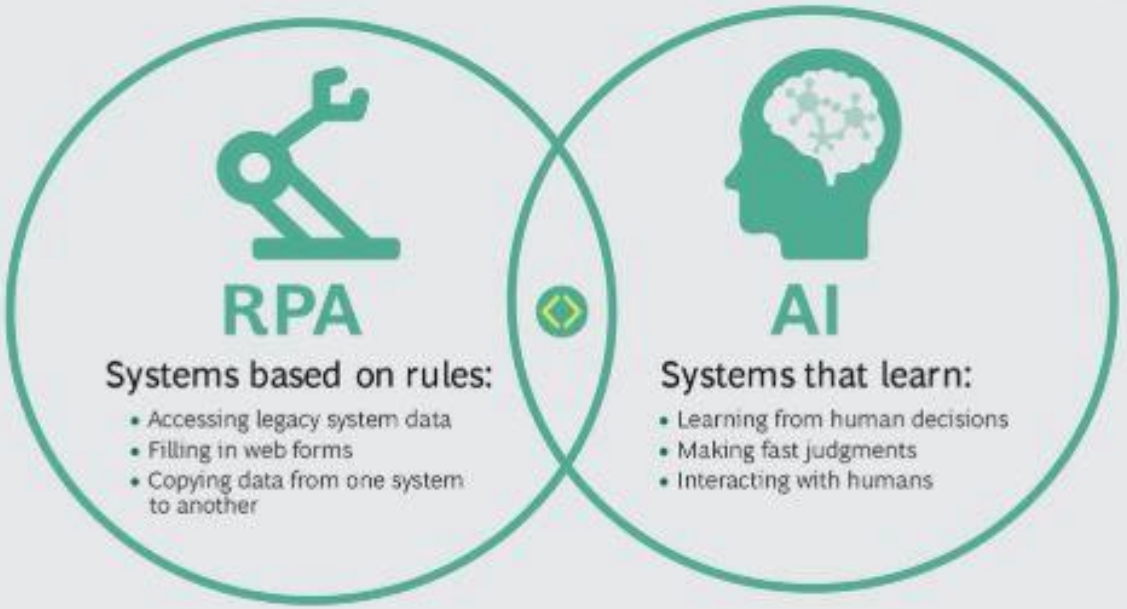




Automation Spectrum



Learning AI trust skills with RPA



Conclusion

- ✓ Great power Competition is Changing how the workforce must operate
- ✓ Human-Machine teaming is inevitable
- ✓ The concept of AI can be daunting and opaque
- ✓ Trust is a key element to wide-spread AI adoption
- ✓ **AI STARTS WITH AUTOMATION**
- ✓ Build Your AI Skillset with existing enterprise RPA
- ✓ A workforce that understands automation will better understand how, when, and where to employ AI to achieve true human-machine teaming capabilities


Telos®