SYSTEMS ENGINEERING RESEARCH CENTER

CENTER FOR COMPLEX SYSTEMS & ENTERPRISES

STEVENS INSTITUTE OF TECHNOLOGY 1870

Research and Application Workshop

AI4SE & SE4AI

Large Language Models in Enhanced Electronic Warfare

Carlo Lipizzi – clipizzi@stevens.edu

September 2024

What is Electronic Warfare

- Electronic Warfare (EW) refers to the use of the electromagnetic spectrum (EMS) to detect, intercept, disrupt, or manipulate enemy communications, radar, and signals
- It includes actions taken to deny the enemy the effective use of the EMS, such as jamming, deception, and spoofing
- EW encompasses Electronic Support (ES) (intercepting signals), Electronic Attack (EA) (jamming and disabling enemy systems), and Electronic Protection (EP) (defending against enemy electronic interference)
- It plays a critical role in modern military operations by providing a strategic advantage in intelligence gathering, defense, and attack through control of the EMS

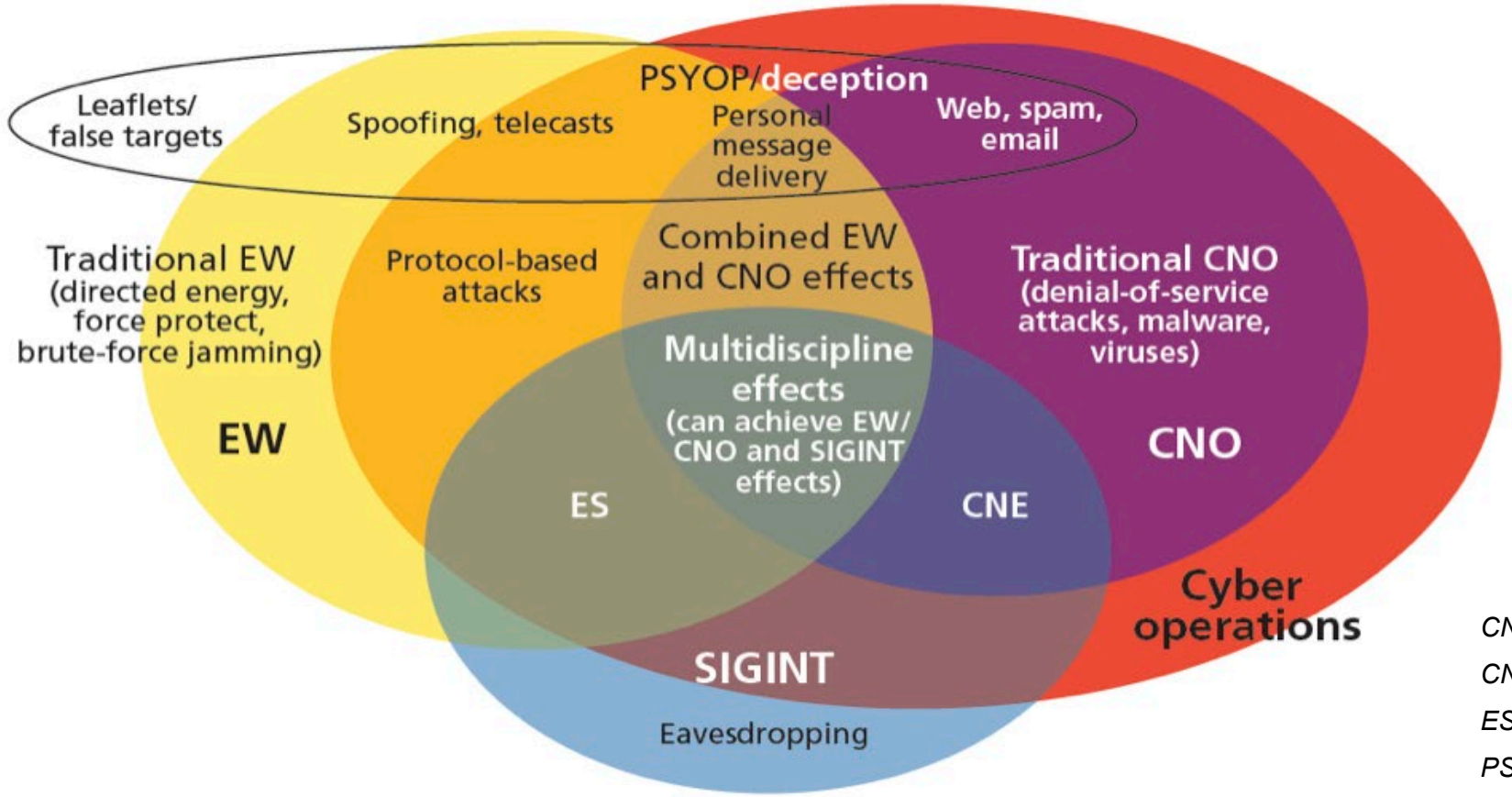
based on: U.S. Naval Institute, JED Online

Signal Intelligence: “beyond” Electronic Warfare

- Signal Intelligence (**SIGINT**) involves the collection, interception, and analysis of electromagnetic signals for the purpose of gathering valuable information from various sources such as communications, radars, and satellite transmissions and is generally considered a subset of Electronic Warfare/Electronic Support
- It is used in military and non-military domains - including cybersecurity, telecommunications, law enforcement, disaster response and emergency management - to monitor and analyze data flow for identifying potential threats, managing resources, or detecting anomalies in communication networks
- SIGINT helps organizations ensure secure communications by detecting unauthorized signals, mitigating interference, and maintaining signal integrity in complex environments
- In fields like disaster management and emergency response, SIGINT can be used to track communications, locate distress signals, and coordinate effective responses through real-time data analysis and communication network monitoring

Electronic Warfare in the Information "Warfare" context

- "Electromagnetic spectrum operations (EMSO) comprise all coordinated (military) actions to exploit, attack, protect, and manage the electromagnetic environment to achieve given objectives"



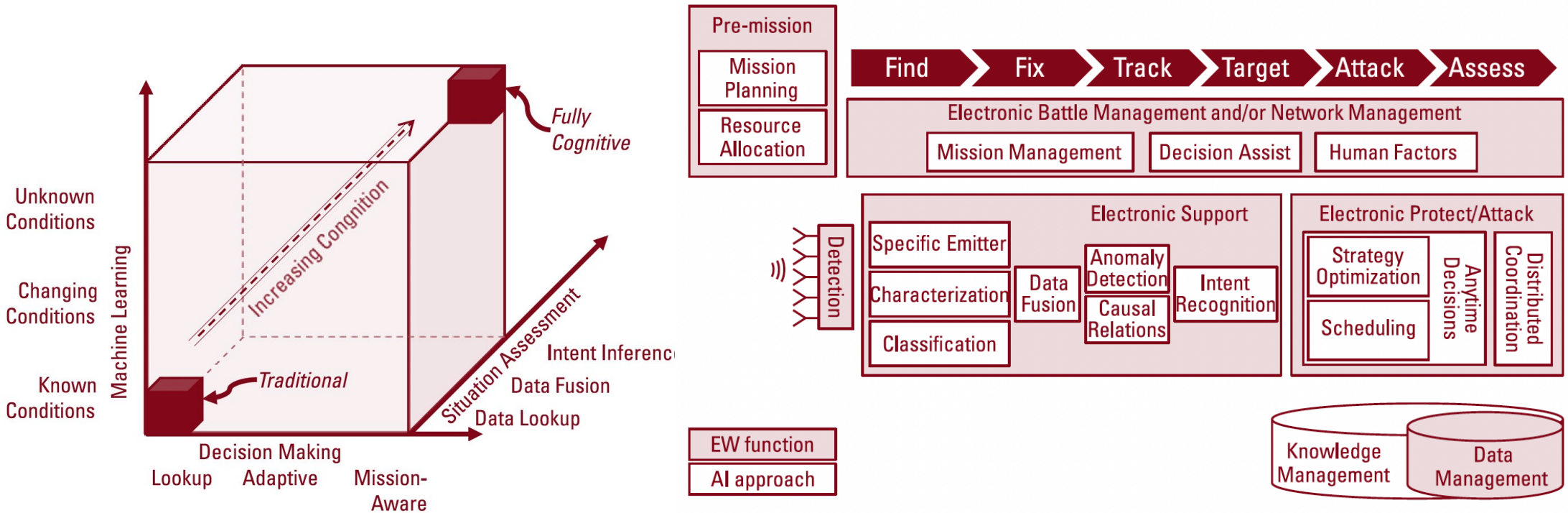
CNE: Computer Network Exploitation;
CNO: Computer Network Operation;
ES: Electronic Surveillance;
PSYOP: Psychological Operations

based on: Porche, et al., "Redefining Information Warfare Boundaries for an Army in a Wireless World"

Data Science in Electronic Warfare

- Big Data Analytics: Leveraged to process large volumes of signal data collected from various sources in the electromagnetic spectrum
- Anomaly Detection: Data science techniques were used to detect unusual patterns that could signify threats, such as new jamming techniques or spoofing attempts
- Predictive Analytics: Early models predicted adversary actions based on historical electromagnetic activity

Cognition in Electronic Warfare



Porche, et al., "Redefining Information Warfare Boundaries for an Army in a Wireless World"

Cognitive Electronic Warfare Systems

- Cognitive EW Systems: AI and machine learning algorithms were integrated into cognitive EW systems, allowing them to adapt to changing environments autonomously
- Reinforcement Learning: Used to dynamically select the best countermeasures in jamming and defense, learning from real-time signals
- Automated Threat Detection: Systems were developed to automatically detect and classify new threats based on signal characteristics

AI for the Defense Applications

- Intelligence, Surveillance, and Reconnaissance
- Cybersecurity
- Autonomous and Unmanned Systems
- Command and Control/Decision Support Systems
- Warfare Simulation and Training
- Weapon Systems
- Information Warfare and Psychological Operations
- Healthcare and Battlefield Medicine
- Electronic Warfare
- Companies such as Palantir Technologies Inc., Anduril Industries Inc., and Microsoft, are either developing AI-based decision platforms for the Pentagon or are already working with the US Defense Department to provide AI solutions [Source: Future Warfare and Critical Technologies – by R. P. Rajagopalan and S. Patil - 2024]
- DoD established in 8/23 a “generative AI” task force - named “Lima” - led by the Chief Digital and Artificial Intelligence Office [DoD 8/10/23]

Early Applications of AI in Electronic Warfare

- SIGINT/Automation of Signal Processing: Early AI models were used to automate the detection, classification, and tracking of electromagnetic signals
- Pattern Recognition: AI helped identify recurring patterns in intercepted signals for faster threat detection and response
- Basic Jamming Techniques: Machine learning was applied to optimize electronic jamming in real-time, adapting to adversary countermeasures
- Training and Simulation: simulating adversarial tactics for training, preparing operators for real-world electronic warfare

Cyber and EW Integration

- AI-Driven Cyber-EW Systems: AI models have been applied to the integration of cyber and EW operations, where AI could process cyber vulnerabilities in electronic systems
- Cross-Domain Threat Detection: Early AI systems enabled detection of cyber threats in EW environments, improving defenses
- Automation in Cyber-Electronic Defense: AI automated the identification of vulnerabilities in EW systems that could be exploited through cyberattacks

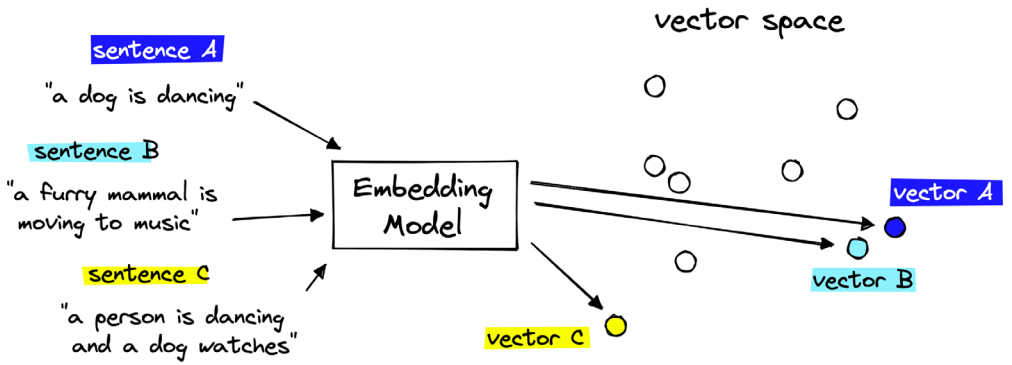
Current “AI” – Large Language Models

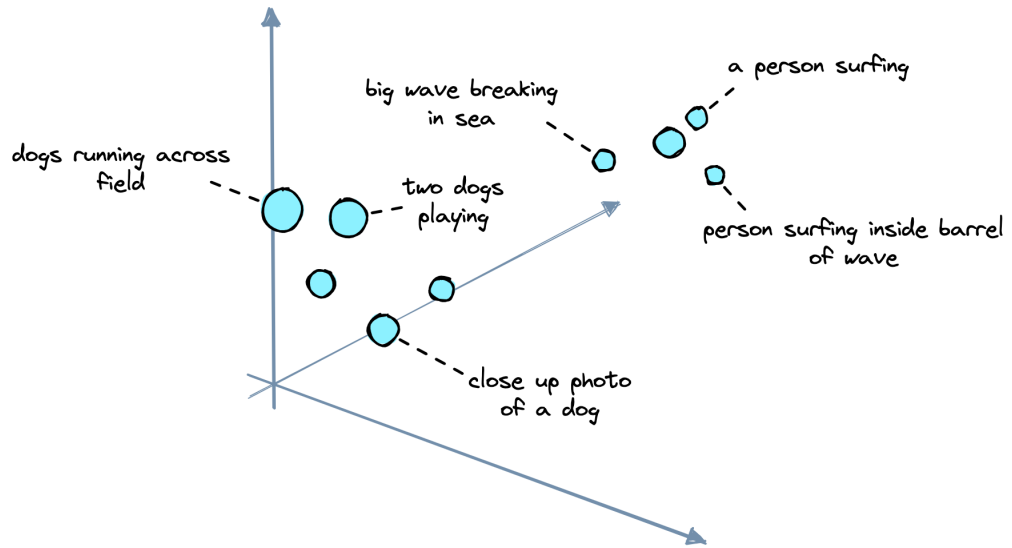
- While “AI” is studied and applied since decades, the type of “AI” we see now is primarily based on Machine Learning, that is a form of representation of “Intelligence” based on getting facts from existing data, with a bottom-up approach
- Without pertinent data – and a lot of it - there is no Machine Learning
- The leading Machine Learning algorithm is “transformer” (created by Google) and it is fully focused on analyzing language, determining and matching patterns in the training data/text and the question from the user

What is in a Large Language Model (LLM)

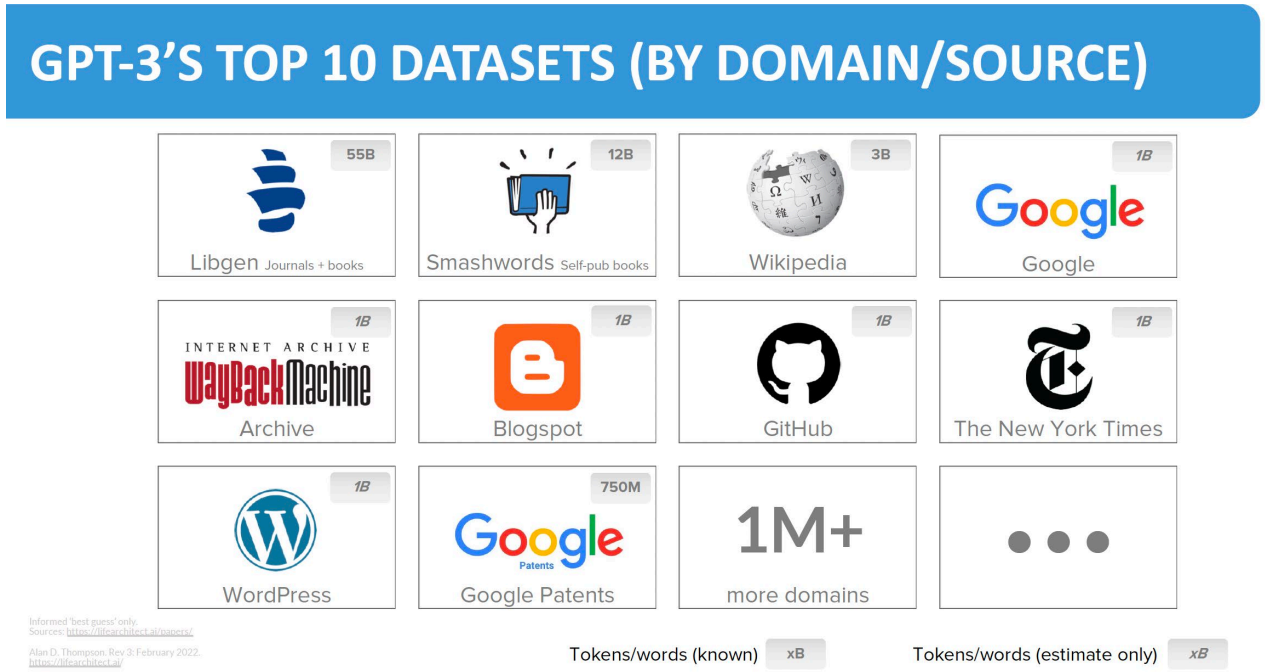
- LLMs are probability-driven pattern matchers with a conversational layer
- They do not “understand” the text
- Being based on data for “reasoning” there is a bias issue
- No traceability of the sources (commercial LLMs)
- Leading/commercial LLMs – like ChatGPT – have limited/no domain-specific knowledge
- High cost of training

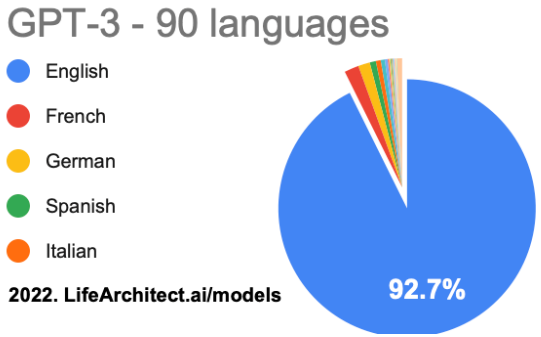
The concept of “proximity” in LLMs





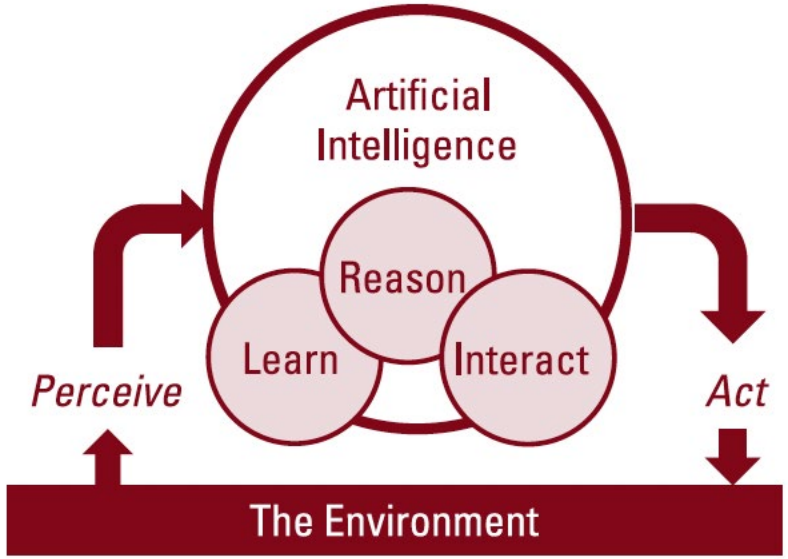
What is in the training data for LLMs





- The total size of the training dataset is estimated in **45TB** of text
- Being a data-driven model, there is an intrinsic bias, induced by the data used for the training
- The estimated cost to train ChatGPT is **$4.6 million** with an estimated energy usage of 936 MWh. This amount of energy is enough to power 30,632 American households for a day, or 97,396 average European households for a day

LLMs in EW



- Signal Intelligence/Electronic Countermeasures
- Real-Time Decision Support
- Dynamic Spectrum Management
- Autonomous Drone Swarms
- Predictive Warfare Models
- Enhanced Cyber-Electronic Warfare Integration

Figure from: Porche, et al., "Redefining Information Warfare Boundaries for an Army in a Wireless World"

Challenges in the use of LLMs

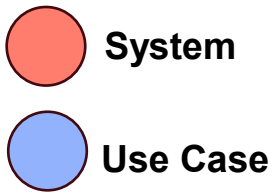
- ML systems and LLMs in particular are based on data. Accurate, real, abundant data is conditio-sine-qua-non for those systems. Data availability in military environment can be problematic. So called “synthetic data” are proved to be ineffective in critical systems
- Bias. Being data-driven, LLMs apply all the intrinsic biases data can have
- Trustworthiness. Quality of data determines the trustworthiness of the system. Limited data, inaccurate data, non domain-specific data would all make the LLM not able to play a role in mission critical situations
- Transparency and interpretability. LLMs are based on deep neural networks, with billions of parameters. There is no way to get a sense of what is happening in the network during execution
- Potential vulnerability to adversarial attacks

Our research on LLMs

- **Custom LLM**. We developed a tutor System for a Course. Creating a custom LLM would give users a better control of the sources, as well as a higher degree of specialization
- **Trustworthiness Evaluation System**. This system assesses how accurately an LLM provides relevant answers within a specific domain, addressing the LLM's "competence" as a measure of trust
- **Plagiarism Detection System.** This system identifies potential plagiarism comparing sentence completions from the LLM with the completion in the actual text to determine similarity and thus the likelihood of plagiarism
- **Bias Detection System.** This system is based on defining "biasers" and measure their presence in the answers from the LLM

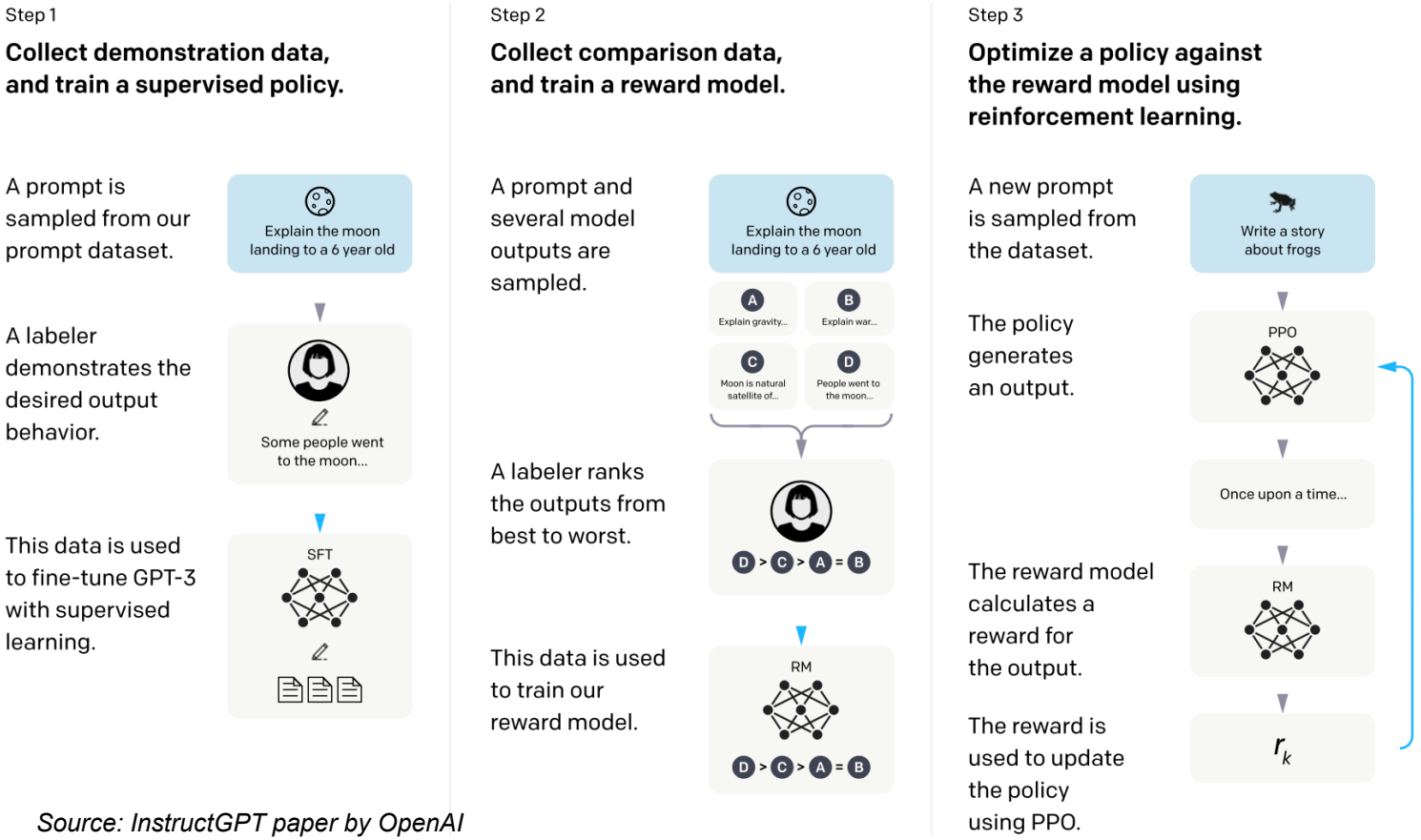
Use Cases - Our research fitting into LLMs for EW

- Due to the reusable approach we used in the developments, application of one of our system to a specific use case could be done in a relatively easy way
- The main issue would be the availability of data to make the system actionable
- Computing resources can be critical for some of the systems



Why creating a LLM is a “System” problem

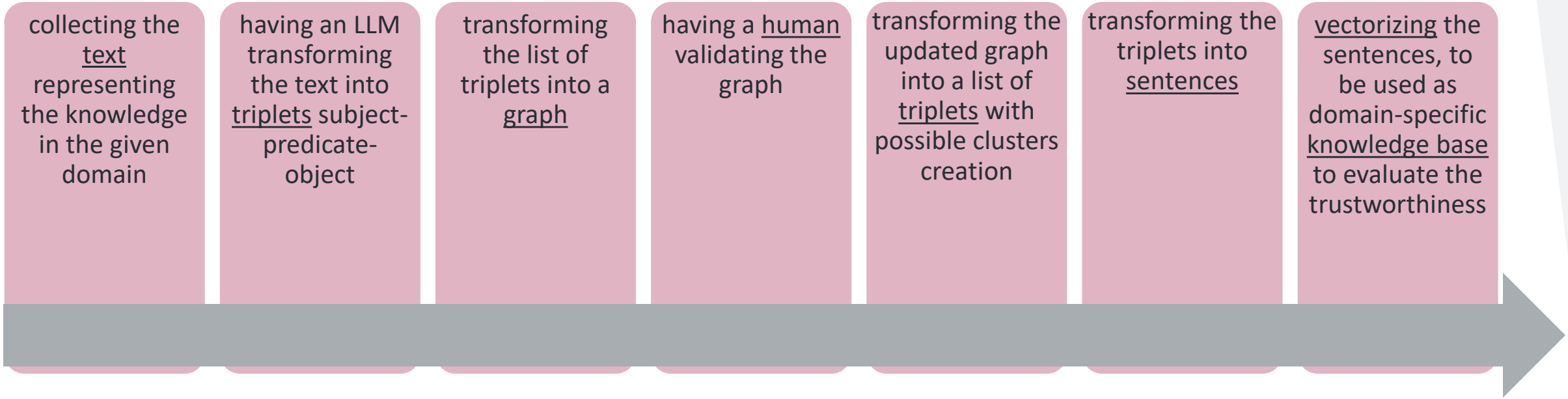
- All the leading LLMs are based on the same model, that is “transformer” (by Google)
- All the leading LLMs using the same vast Open Source text (with some exceptions discussed in courts…)
- The difference is in the process for training and – with less relevance – the usability



Source: InstructGPT paper by OpenAI

Why using an LLM is a “System” problem

- LLMs and AI in general is not a tool issue: no LLM can fully address a complex problem
- Designing processes/pipelines is more and more the way to go in AI applications. Humans in the loop is also happening
- The following is an example of the process we design and implement in one of our systems (Trustworthiness Evaluation System)



CENTER FOR COMPLEX SYSTEMS & ENTERPRISES

STEVENS
INSTITUTE OF TECHNOLOGY
1870

*THANK **YOU***

Stevens Institute of Technology
1 Castle Point Terrace, Hoboken, NJ 07030
clipizzi@stevens.edu