ARTIFICIAL INTELLIGENCE EXPANSION, A TRANSFORMATION OR A MUTATION

Ali Rah

ABSTRACT

The field of Artificial Intelligence (AI) is evolving in a fast pace impacting a wide range of other field including general public use of social media platforms all the way to industrial activities and Cybersecurity. When AI is combined with Quantum Computing the abilities of AI are exponentially increased. This paper aims to explore the evolution of AI, discuss if this evolution a transformation or a mutation, and its correlation with Quantum Computing. It is also looking into the impact of AI on Cybersecurity risks and mitigation.

KEYWORDS

Artificial Intelligence, Quantum Computing, Cybersecurity, Deep Learning, Machine Learning.

1. INTRODUCTION

Artificial Intelligence, AI, in short, is an expression to which we have been exposed daily for the past couple of years, especially since the introduction of the ChatGPT. Many words and terms are included in conversations when talking about AI, such as “Deep Learning”, “Machine Learning”, “Automation”, “Algorithm”, “API”, “Big Data”, “Chatbot”, “Cognitive computing”, “Data mining”, “Generative AI”, “Neural network”, “Pattern recognition”, “Predictive analytics”, “Quantum computing”, and, of course, “ChatGPT”, in addition to more other terms [1]. There is this feeling that, sometimes, these expressions are forced into a conversation only to show that the speaker is up to date with what’s happening or to bring attention to potential dangers/challenges brought by AI without exactly knowing what these are.

So, is this apparent exponential expansion of AI another step in the evolution of the associated technology? Or is it a jump/mutation, skipping many steps in the evolution process, in technology that even the most up-to-date professionals will find challenges in keeping up with the pace?

The release and the fast pace of ChatGPT 1, 2, 3, 4, 5, … seems to mark a turning point. It tends to be somewhat equivalent to humans being, finally, left behind by algorithms. AI is the new solution but, at the same time, the biggest threat. Questions are raised about humans' ability to understand and follow what’s happening.

So, is it the time when robots can think by themselves, adapt to different situations, make their own decisions (right or wrong), find their own sources of energy, take over other systems to survive or to expand, and launch their own defensive means? Or, is the human brain within the human body still a goal on the horizon to near but never reach? Is AI at the level of the human mechanism triggered by a visual alert transferred to the brain that launches a spark of adrenaline, associated with an increase in heart rate, increased breathing, a punch of energy produced by the liver, a muscular system synced with sympathetic and parasympathetic systems, to execute a lifesaving action in a fraction of a second?

DOI: 10.5121/ijcsitce.2024.11302

2. EVOLUTION/TRANSFORMATION VS MUTATION

Before diving into the world of artificial intelligence, let's start by exploring the differences between evolution/transformation and mutation processes.

A mutation is a "profound and radical change," as described by the "Centre National de RessourcesTextuelles et Lexicales" (CNRTL) [2]. On the other hand, evolution is "a process that results in changes … over time" [3]. The key here is time; a mutation happens over a relatively short time compared to evolution.

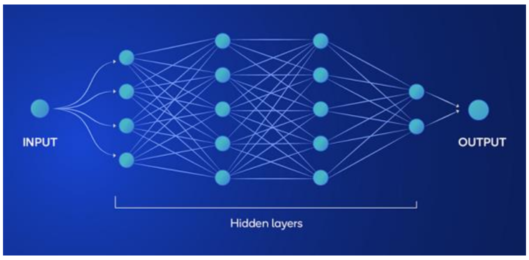
In the world of genetics, mutations are essential events in the process of evolution. "Without mutation, evolution could not occur." [4]. Mutations are not always synonyms of negative events. They could be beneficial, neutral, or have a negative impact.

Philippe Droz-Vincent explains that "political history is made up of continuities broken by major events (revolutions, coups d'état, transitions, ruptures within a regime, political crises, etc.). But the social data on which political interactions are built, as the basis for the relationships on which political life is based, undergo constant evolution and end up generating discontinuities." [5, pp. 75-109]

A mutation in the context of this paper is an unexpected event that happens over a relatively short period of time, is triggered by a new discovery, and takes the knowledge many steps forward. On the other hand, transformation/evolution is the continuous process of advancement of human knowledge based on theories, studies, research, tests, trials, results, and putting these results into practice.

3. DEFINITION OF ARTIFICIAL INTELLIGENCE

There are many different definitions of AI depending on the audience, such as the general public or a community of scientists. The definition of AI seems to change over time. It was, before 1950, without calling it "AI", about how to build an "Artificial Brain" or a "Robot". It moved to building algorithms to make machines execute repetitive tasks faster (than humans), with fewer human concerns such as fatigue. Later, this concept was about big data, data mining, looking for patterns, making complex calculations, and solving problems based on predefined paths, following a preprogrammed human logic (basically, the "If-Then" loop in an advanced format). AI was and continues to be trained on the exponentially growing publicly available data, proprietary data, and data gathered from sensors.



Neural Network. Source: Qualcomm [6]

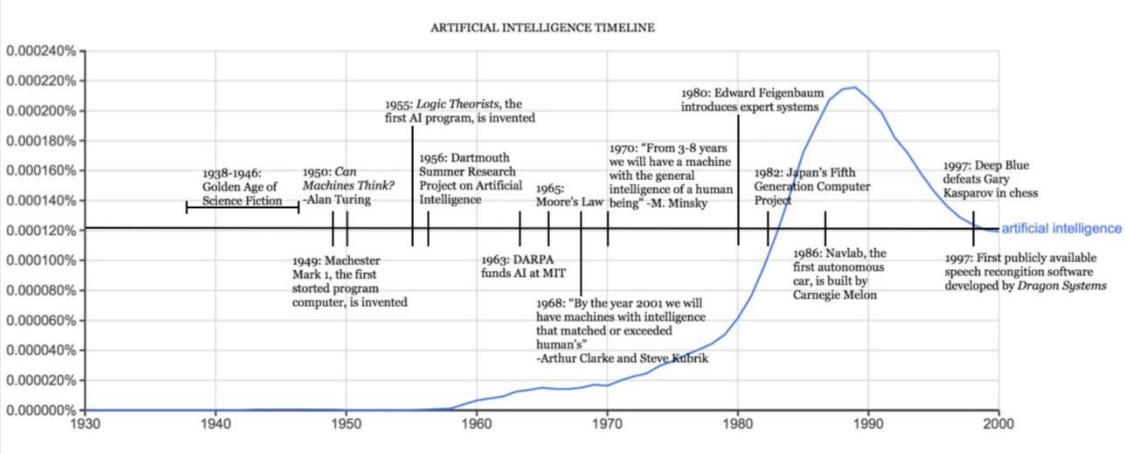
Note: Many aspects of AI (Machine learning , deep learning …) are based on "Input" (Data) given to a "Machine" which process it in layers transparent to users and presents an "Output" as a result at the disposal of users.

IBM defines AI as a “technology that enables computers and machines to simulate human intelligence and problem-solving capabilities.” [7]. Britannica defines AI as “the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings. The term is frequently applied to the project of developing systems endowed with the intellectual processes characteristic of humans, such as the ability to reason, discover meaning, generalize, or learn from past experience.” [8]. The University of Illinois Chicago defines AI as “a branch of computer science that aims to create machines capable of performing tasks that typically require human intelligence. These tasks include learning from experience (machine learning), understanding natural language, recognizing patterns, solving problems, and making decisions. From self-driving cars to virtual personal assistants, AI is reshaping various aspects of our daily lives, and its significance continues to grow.” [9]

The shared principle between these definitions is the idea of “human intelligence”. The main goal of AI is to mimic the human ability to understand natural language, reasoning, solving problems, and making decisions.

4. HISTORY OF ARTIFICIAL INTELLIGENCE

The expression “Artificial Intelligence” was first used around the 1950s. The term was introduced by Stanford Professor John McCarthy in 1955 and defined as “the science and engineering of making intelligent machines”. [10].



Source: Harvard University [11]

Note: This timeline shows the history of AI since early 1900s. It highlights a steady evolution with time to time acceleration and back to linear progress

Alan Turing, a young British polymath, explored the mathematical possibility of “Artificial Intelligence”. In 1950, he suggested that “humans use available information as well as reason in order to solve problems and make decisions, so why can’t machines do the same thing?” [12]

In 1956, the Dartmouth Summer Research Project on Artificial Intelligence (DSRPAI) historic conference hosted by John McCarthy and Marvin Minsky presented what was considered by many to be the first “Artificial Intelligence” program. The conference fell short as there was a failure to agree on standard methods for the field. [13]

Between 1957 and 1974, AI transformation was progressing. Computers could store more information and became faster, cheaper, and more accessible. Many machine learning algorithms, such as Newell and Simon’s General Problem Solver and Joseph Weizenbaum’s ELIZA, have also improved. Government agencies such as the Defense Advanced Research Projects Agency (DARPA) started to fund AI research at several institutions. [13]

In 1980, Expert Systems were created and programmed to copy the decision-making ability of a human expert. The latter would answer questions that would be used in expert situations, and AI would learn every single possibility. In 1997, IBM’s Deep Blue Supercomputer beat Gary Kasparov, the world chess champion. It became the first computer to beat a human in chess. Speech recognition software was implemented on Windows that same year, and in 2011, Apple released a similar software named “Siri”. [14]

In 2003, NASA landed two rovers on Mars (Spirit and Opportunity), and they navigated the planet's surface without human intervention. This event was considered, among others, between 1993 and 2011 an agent of AI, bringing more interest to the topic but also more funding. In 2006, companies like Twitter, Facebook, and Netflix started utilizing AI in advertising. Later in 2012, Jeff Dean and Andrew Ng, from Google, trained a neural network to recognize cats by showing unlabeled images and no background information to this network. Many other events in the following years led to the creation of the first human-looking robot, which could show some realistic human appearance and emotions. In 2020, OpenAI launched beta testing GPT-3, using Deep Learning to create code, poetry, and other such language and writing tasks, content almost indistinguishable from those produced by humans. [15]

GPT-3 and Gato, released by DeepMind in 2022, pushed AI capabilities to new levels. However, they were based on Large Language Models (LLMs), which, in 2018, were trained on vast quantities of unlabeled data. These LLMs became the foundation models that can be adapted to various specific tasks. Many of the latest LLMs, such as Llama 2, GPT-4, and BERT, use the relatively new neural network architecture called Transformer, which was introduced in 2017 by Google. [6]

5. GENERATIVE AI

“Generative AI”, along with “ChatGPT”, are among the most used terms in the last couple of years. Generative AI represents a development in the field. Rather than merely responding to input, the system processes data. It generates unique content using predictive algorithms, which are essentially a series of sequential instructions. When an AI chatbot like ChatGPT or Google Bard produces original poetry, songs, scripts, and other works, it might be considered content for a large language model (LLM). The word "large" in LLMs refers to the vast amount of data the language model was trained on. The result gives the impression that the computer is expressing itself artistically. Still, in reality, it is only making predictions about a group of tokens (the building blocks of text that a chatbot uses to process and generate a response) and choosing one of them. [16]

AI is not yet at the Artificial General Intelligence (AGI) level. AGI remains a speculative concept. AGI systems would mimic or even exceed human intelligence, in contrast to generative AI, which appears to be capable of some human-like tasks. Robots would develop awareness and become self-aware.

Baum and Villasenor underlined that there is no single, formally recognized definition of AGI. “…highly autonomous systems that outperform humans at most economically valuable work”

(OpenAI's charter), "[a] hypothetical computer program that can perform intellectual tasks as well as, or better than, a human." (Hal Hodson, in The Economist), "…any intelligence (there might be many) that is flexible and general, with resourcefulness and reliability comparable to (or beyond) human intelligence." (Gary Marcus), and et al. "…systems that demonstrate broad capabilities of intelligence, including reasoning, planning, and the ability to learn from experience, and with these capabilities at or above human-level." (Sébastien Bubeck et al) are some given examples to define this concept. [17]

It is essential to highlight that AI might be inaccurate. LLMs such as Bard and ChatGPT occasionally experience hallucinations (a situation where an AI system produces fabricated, nonsensical, or erroneous information). When a user enters a prompt, the system might fabricate a response that isn't accurate in any manner. Occasionally, the response is merely unreliable. The material is provided authoritatively and confidently, further complicating issues because it sounds and looks genuine. [16]

6. ARTIFICIAL INTELLIGENCE AND QUANTUM COMPUTING

Artificial intelligence discussions also go through the concept of "Quantum computing" and how it could make the evolution of AI a mutation rather than a transformation.

Stackpole defines quantum computing as "an innovation most can't define and still don't properly understand, might be the next obscure technology to have a seismic effect on business." [18]. This seismic effect is indeed the concept of mutation defined earlier in this paper. It is also not easy to define, nor to understand, as quantum computing is based on quantum physical, a deep and theoretical field based on the state of the matter switching between classical states (solid, liquid, gas …) to quantic-states defined by waves, frequencies, and probabilities.

The principles of quantum physics are used in quantum computing to simulate and resolve complicated issues that are too challenging for the present generation of classical computers. "Classical" computers, even the fastest ones used nowadays, are all based on the simple entity, the "Bit". The bit could have only two values, "0" or "1", making it the industry of "Zeros" and "Ones". It's based on an electrical circuit that could be either "Closed", meaning the light is "On", meaning the value of the bit is "1"; or this electrical circuit is "Open", meaning the light is "Off", and, therefore, the bit has a value of "0".

Quantum computers are based on a totally "new" (quantum physics goes back to the year 1900[19]) concept of the "Quantum Bit" (QuBit), subatomic particles, which no longer hold a discrete value of "1" or "0" but has a value "between 0 and 1" in a continuum based on a certain probability. There is nothing certain here.

As an example, in quantum mechanics, particles, such as electrons and protons, continuously switch between the states of "solids" and waves. This switch could be visualized as an electron flying like a golf ball switching, at high speed, to a sound wave that we could hear but not see. The challenge in this concept is how to "maintain" the state of such "entities". We now master how to assign a value to a bit (0 or 1) and keep it that way as long as we want or as needed. However, how do we assign a value to a Qubit close to 0 or 1 (as it depends on the probability of having a value)? How to maintain the Qubit at this value and for how long (which means a known value at a point in time, which means "Memory", the base of any computing process)? How do you put these Qubits "physically" in a box (Quantum Computer) and use them for any purpose?

Apparently, we are not yet where we want to be, despite more than a century since quantum physics saw the light. Scientists are able to control about a thousand Qubits, which is a great achievement on the road to quantum computing. Osprey, a 433-qubit machine, was launched by IBM last year, on building a 100,000-qubit machine within 10 years. Instead of dealing with waves and the associated challenges, or the need to bring particles to a “relatively” high speed, scientists are working with low temperatures, as near as possible to Zero Degrees Kelvin (Absolute Zero), where particles in metals adopt a “quantic behavior” while still in a “classic state”. As such temperatures, it is possible to maintain the status of a Qubit. This means that a quantum computer doesn’t look any closer to what we are used to. A quantum computer is based on powerful cooling abilities. It is based on the concept of “Supra-Conductivity”, which makes its size and shape different in size and shape.

Quantum Computer. Source: Barron’s [20]

Note: The structure of a Quantum Computer as a Chandelier suspended in the middle of the room is nothing close to computers used on a daily basis at home and for work

Artificial intelligence is mainly based on computers’ speed in processing huge amounts of data. Quantum computing, when “tamed,” could be a jump/mutation in the evolution of AI. In addition to the potential speed, the Qubits can hold, in theory, many states simultaneously, exponentially increasing computer processing power and memory abilities.

7. Artificial Intelligence and Cybersecurity

In the field of cybersecurity, both artificial intelligence and quantum computing keep InfoSec professionals awake at night. They both raise concerns about bringing more powerful tools to malicious actors' disposal, targeting information and information systems. These concerns are not new. They are inherent to the evolution of technology. Each and every advancement brings new concerns, questioning countermeasure abilities to detect vulnerabilities, apply efficient controls, and defend organizations’ assets.

When an artificial intelligence “abrupt” advancement, such as generative AI, is perceived as a mutation in what is available for black hats to attack information systems, it is a healthy reaction from InfoSec professionals to consider that a wake-up call to check systems attack surface, update security controls, and improve defense in depth. It is also crucial to bring management, leadership, and C-Suite up to date with the status of the organization's security.

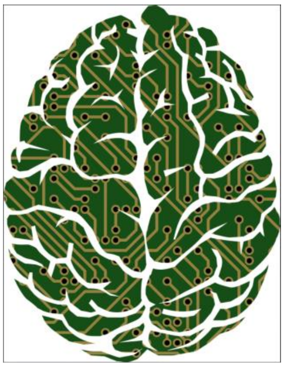
On the other hand, while serving black hats, AI and quantum computing also bring new tools to defend organizations' perimeters better. Quantum computing is already allowing the building of encryption keys that are, until now, practically unbreakable. The process to take the desirable action differs between black and white hats. The formers are motivated by the quick return of their actions, targeting different types of organizations (ransomware, social engineering …) and generating huge profits, as cybercrime is becoming a standalone industry with budgets surpassing the budget of entire countries. Black hats also need to find a single vulnerability to exploit in order to reach their goal. The latter, white hats, have to go through a long process to secure the necessary budgets needed to secure organizations' assets. They must secure senior management approval, go through administrative and financial processes, acquire/develop security controls, and apply them. They must also enforce these controls, protect ALL assets, and accept the residual risk.

8. CONCLUSION

Artificial intelligence is a decades-old concept. Development teams are continuously improving their abilities, empowered by the open concept, providing teams working worldwide around the clock and sometimes giving the perception of the advent of a jump/mutation in this continuous transformation.

Artificial intelligence is a reality that already impacts every single field (healthcare, energy, environmental systems, innovative materials …), from using ChatGPT to chat over social media to influencing decision-making in very sensitive areas. It brings many advantages when using deep learning, machine learning, and other tools. However, it brings risks related to how algorithms are built, of "good" decisions based on "efficient" systems providing outputs that look genuine and "therefore, correct".

The concept of Artificial General Intelligence (AGI) has already been introduced as the next level of AI. The key here is the primary goal of mimicking human intelligence. The following representations symbolize this nuance. On one side, AI is represented with discrete connections using electronic circuits. In contrast, the other side represents a human brain with its continuum of matter composed of neurons, neural connections, but also this gray and white matter in between. Despite all the advancements in knowledge, the human brain is still a mystery with many unexplained abilities.



Source: Pixabay[21]

Source :Africanian[22]

Note: AI is aiming at mimicking human intelligence by building systems to work like human brain. The continuum structure and the complex functions of the brain are great goals to reach

Continual changes in architectures, algorithms, and techniques will continue impacting the ongoing AI research. There will be forward jumps from time to time, bringing new advancements and introducing new tools. However, the progress of the process as a whole will still be looked at for out of the box, a continuous transformation, advancing one (or a few) step (s) at a time.

9. FUTURE RESEARCH

Continuous monitoring of AI’s achievements and how close it is from human intelligence could bring more papers about the benefits of AI, of quantum computing, but also about the new risks and challenges, especially in the field of cybersecurity.

REFERENCES

[1] Coursera, "Artificial Intelligence (AI) Terms: A to Z Glossary," 19 March 2024. [Online]. Available: https://www.coursera.org/articles/ai-terms.

[2] CNRTL, "Definition Mutation," [Online]. Available: https://www.cnrtl.fr/definition/mutation.

[3] Nature, "Definition Evolution," [Online]. Available: https://www.nature.com/scitable/definition/evolution-78/.

[4] Berkeley, "DNA and Mutations," [Online]. Available: https://evolution.berkeley.edu/dna-and-mutations/.

[5] P. Droz-Vincent, "Les Mutations des Societes et leurs Consequences Politiques," 2004. [Online]. Available: https://www.cairn.info/moyen-orient-pouvoirs-autoritaires-societes-bloque--9782130547167-page-75.htm.

[6] P. Lawlor and J. Chang, "History of AI: How generative AI grew from early research," 22 August 2023. [Online]. Available: https://www.qualcomm.com/news/onq/2023/08/history-of-ai-how-generative-ai-grew-from-early-research.

[7] IBM. [Online]. Available: https://www.ibm.com/topics/artificial-intelligence.

[8] B. J. Copeland, "Artificial Intelligence," 29 April 2024. [Online]. Available: https://www.britannica.com/technology/artificial-intelligence.

[9] U. o. I. C. UIC, "What Is (AI) Artificial Intelligence?," 25 March 2024. [Online]. Available: https://meng.uic.edu/news-stories/ai-artificial-intelligence-what-is-the-definition-of-ai-and-how-does-ai-work/.

[10] C. Manning, "Artificial Intelligence Definitions," September 2020. [Online]. Available: https://hai.stanford.edu/sites/default/files/2020-09/AI-Definitions-HAI.pdf.

[11] U. Harvard, August 2017. [Online]. Available: https://i0.wp.com/sitn.hms.harvard.edu/wp-content/uploads/2017/08/Anyoha-SITN-Figure-2-AI-timeline-2.jpg.

[12] R. Anyoha, "The History of Artificial Intelligence," 28 August 2017. [Online]. Available: https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/.

[13] Harvard, "History of Artificial Intelligence," 2017. [Online]. Available: https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/.

[14] Y. Sanchez, "The History of Artificial Intelligence," 20 Octobre 2022. [Online]. Available: https://medium.com/@20yael.sanchez/the-history-of-artificial-intelligence-27f0d62f95c7.

[15] Tableau, "What is the history of artificial intelligence (AI)?," [Online]. Available: https://www.tableau.com/data-insights/ai/history.

[16] R. Ghani, "Artificial Intelligence Explained," July 2023. [Online]. Available: https://www.heinz.cmu.edu/media/2023/July/artificial-intelligence-explained.

[17] J. Baum and J. Villasenor, 18 July 2023. [Online]. Available: https://www.brookings.edu/articles/how-close-are-we-to-ai-that-surpasses-human-intelligence/.

[18] B. Stackpole, "Quantum computing: What leaders need to know now," 11 January 2024. [Online]. Available: https://mitsloan.mit.edu/ideas-made-to-matter/quantum-computing-what-leaders-need-to-know-now.

[19] D. Styer, "A Brief History of Quantum Mechanics," 1999. [Online]. Available: https://www2.oberlin.edu/physics/dstyer/StrangeQM/history.html#:~:text=He%20announced%20this%20result%20on,one%20found%20it%20particularly%20significant..

[20] E. J. Savitz, "Quantum Computing Will Change the World. How to Play the Stocks.," 27 November 2022. [Online]. Available: https://www.barrons.com/articles/quantum-computing-stocks-51669248235.

[21] Pixabay, "Free images of Artificial Intelligence," [Online]. Available: https://pixabay.com/images/search/artificial%20intelligence/?.

[22] Africanian, "South Africa harnesses artificial intelligence, machine learning in Covid-19 fight," [Online]. Available: https://africanian.com/business/south-africa-harnesses-artificial-intelligence-machine-learning-in-covid-19-fight/.

AUTHOR

Dr. Ali Rah has over 30 years of experience in different fields related to security (Physical, Building, Staff, Electronic, Information, Access control, Law enforcement, Legal policies, …). He holds a Master in Cybersecurity and a Doctorate in Information Assurance. He also holds different security certifications including CISSP, CompTia Security +, and AWS Cloud Foundations.