인공지능과 사이버보안

水魚之交

2020.11.19.(목)

김 인 중

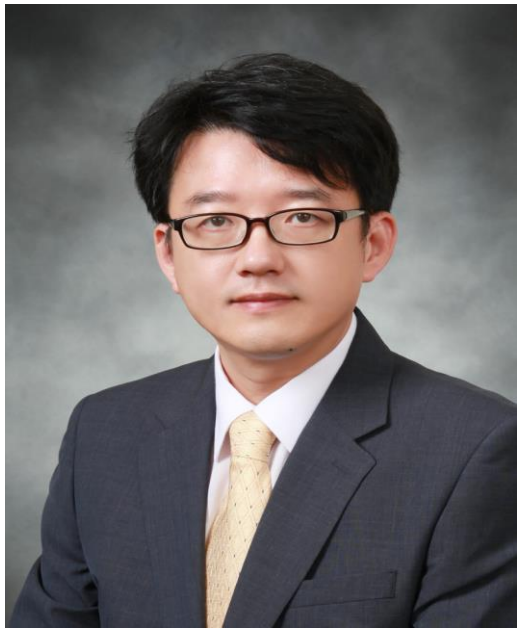
강사 소개

현 : 사이버안전훈련센터 교수

국가보안기술연구소 부소장

국가보안기술연구소 정책실장

국방과학연구소 선임연구원



한국정보보호학회 부회장

사이버보안보법정책학회 부회장

개인정보보호법학회 정보이사

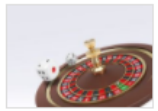
수상 : 국민포장, 경제부총리상, 과학기술부장관상, 국가정보원장상 등

저서 : 스테가노그래피, DMZ, 역사 속의 사이버보안, 탈린 매뉴얼(번역서) 등

보안뉴스 연재 칼럼 [인간의 영역을 넘어서…]

[스토리텔링으로 이해하는 AI 보안-21] 악성 댓글과 인터넷 윤리
내가 게시한 글에 누군가가 욕설과 함께 내 개인 생활 관련 내용을 적어놓았다. 곧 그 내용이 사실인 양 사이버공간에 급속히 퍼지더니 각종 포털사이트와 그룹 채팅,... 권준 기자 | 2020년 11월 08일 21:40

[스토리텔링으로 이해하는 AI 보안-20] 딥페이크(Deep fake)와 가짜뉴스
화상채팅용 전화벨이 울렸다. 스마트폰을 열어보니 아침에 학교 간다고 부리나케 가방 메고 나간 아들 철수다. 평상시에는 대화하자고 해도 볼퉁거리던 녀석이 웬일로 연... 권준 기자 | 2020년 11월 01일 23:04



[스토리텔링으로 이해하는 AI 보안-19] 신과 주사위놀이, 양자암호통신
창조론과 진화론, 천동설과 지동설. 인간은 끊임없이 신의 영역을 향해서 진보해왔다. 인간이 자연의 섭리를 이해하기 시작하면서 기존에 자신들이 믿었던 부분들이 하나... 권준 기자 | 2020년 10월 25일 21:43

[스토리텔링으로 이해하는 AI 보안-18] 여성과 사이버보안
인간의 본능에 의해 그들의 자식들이 태어나고, 그럼으로써 번식했다. 그러다보니 비옥한 토지와 따스한 환경에서 모두가 지내는 게 어려워지기 시작했다. 강한 자와 약... 권준 기자 | 2020년 10월 18일 22:53

[스토리텔링으로 이해하는 AI 보안-17] 블록체인과 비트코인
인간의 문명이 발전하면서 점차 인간은 발품을 팔며 돌아다니지 않아도 모든 일을 다 할 수 있게 되었다. 사이버공간에서 말이다. '디지털혁명의 아이콘'이라고 불리는... 권준 기자 | 2020년 10월 11일 22:25

[스토리텔링으로 이해하는 AI 보안-15] 이데아와 사이버공간
신들과 영웅들이 개입한 트로이 전쟁이 끝난 뒤, 인간 세상에도 많은 변화가 나타났다. "모든 사물에는 신들이 깃들어 있고, 그 신들을 섬겨야 행복해진다"고 믿었던... 권준 기자 | 2020년 09월 28일 00:06

[스토리텔링으로 이해하는 AI 보안-13] 인공지능과 사이버훈련
결국 보안 인력의 교육·훈련은 인공지능 시스템의 고도화·보편화 증대에 지대한 공헌을 한다. 앞으로 한국에서도 인공지능 분야의 교육은 대학은 물론 초·중·고등학교에... 권준 기자 | 2020년 09월 13일 23:33

[스토리텔링으로 이해하는 AI 보안-12] 인공지능과 데이터셋
인공지능 시스템을 활성화시키려면 해당 시스템을 안전하게 적용해볼 수 있는 테스트베드와 데이터셋을 만들어야 한다. 예를 들어, 자율주행 자동차·헬스케어·에너지 등 ... 권준 기자 | 2020년 09월 07일 11:46

[스토리텔링으로 이해하는 AI 보안-11] 보안 샌드박스와 보안산업 육성
최근 제도권에서 인공지능에 대한 관심이 높아지면서 규제 샌드박스에 대한 논의가 활발하게 이루어지고 있다. 하지만 아쉽게도 보안이 함께 고려되고 있지는 않다. 결국... 권준 기자 | 2020년 08월 28일 10:51

[스토리텔링으로 이해하는 AI 보안-9] 파이썬과 오픈소스 취약점
인공지능 프로그램을 개발하는 과정에서 이러한 오픈소스를 이용하는 데 따른 책임 범위를 어떻게 정해야 할지가 또 하나의 숙제로 남았다. 물론 이러한 숙제를 방치한다... 권준 기자 | 2020년 08월 14일 11:42

[스토리텔링으로 이해하는 AI 보안-8] 팬데믹과 기반시설 보호
사이버공간에서 벌어지는 판데믹은 지금 우리가 겪고 있는 판데믹과는 비교가 되지 않을 정도로 엄청난 피해를 유발할 것이다. 다들 느끼다시피 현실에서의 판데믹은 마스... 권준 기자 | 2020년 08월 07일 18:22

[스토리텔링으로 이해하는 AI 보안-6] 위치 정보와 암호 알고리즘
GPS의 예에서 보듯이 인공지능 시스템 설계 시 암호 알고리즘과 같은 보안 대책도 함께 고려해야 할 것이다. 즉, 인공지능 시스템을 개발하면서 실용성만 고려하지 ... 권준 기자 | 2020년 07월 21일 13:05

[스토리텔링으로 이해하는 AI 보안-5] 자명고와 사이버위협 인텔리전스
달빛도 별빛도 구름에 가려 칠흑같이 캄캄한 새벽. 뭔가를 응시하고 있던 한 여인의 손에는 날카로운 은장도가 들려있었다. 잠시 망설이던 그녀는 뭔가를 심한 듯 커다... 권준 기자 | 2020년 07월 10일 13:25

[스토리텔링으로 이해하는 AI 보안-4] 백설 공주와 보안 신뢰성 검증
거울인 나를 물끄러미 바라보는 한 여인을 나는 보고 있다. 그 순간 나르시시즘에 빠진 그 여인에 대한 안쓰러움이 밀려왔다. 자신의 모습에 빠져 다른 여인들과의 끊... 권준 기자 | 2020년 07월 03일 13:55

[스토리텔링으로 이해하는 AI 보안-3] 판도라의 상자: 신뢰성(Confidentiality)=기밀성
판도라의 상자와 관련하여 여러 이야기들이 구전으로 전해 내려오고 있다. 그중 어느 전설에 의하면, 희망과 함께한 것들 중에 Confidentiality도 함께 있... 권준 기자 | 2020년 06월 26일 14:48

[스토리텔링으로 이해하는 AI 보안-2] 퀴베르네테스, 인공지능=사이버
'퀴베르네테스'는 지금 우리가 일상적으로 사용하고 있는 단어인 '사이버(cyber)'의 어원이기도 하다. 미국의 노버트 위너(Norbert Wiener) 교수는 ... 권준 기자 | 2020년 06월 19일 11:04

16회 – 신이라 불린 인간 : 폰 노이만과 앨런 튜링

존 폰 노이만과 앨런 튜링으로 인해 시작된 컴퓨터와 인공지능 이야기
인공지능과 사이버보안은 도저히 뗄 수 없는 관계, 함께 갈 수 있는 정책 마련해야

[보안뉴스= 김주원 사이버보안 분야 칼럼리스트] 트로이 전쟁이 끝나자 인간세계에는 많은 변화가 나타나기 시작했다. 대표적인 예로, 그리스에서 트로이까지 항해하면서 경험을 쌓은 인간들이 그리스의 앞바다인 에게 해에서 사람과 곡식을 운송하던 작은 배는 물론, 거대한 지중해를 항해하며 다양한 물건들을 잔뜩 싣고 무역하는 큰 배도 몰기 시작한 것이다. 트로이 전쟁에서 패한 트로이 왕족 중 일부는 그러한 큰 배에 수많은 유민들을 태우고 대양을 건너 이탈리아 반도의 팔라티노 언덕으로 이주해 로마를 건국하기까지 했다.

[이미지=utoimage]

항해할 때 해안선을 맨눈으로 식별하면서 이동하는 경우에는 위치 파악에 기계의 도움이 필요하지 않다. 하지만 보이는 건 하늘과 물뿐인 망망대해를 항해해야 하는 상황에서는 위치 파악 수단이 필요하다. 이를 위해 태양의 위치, 별의 움직임, 바람의 세기, 파도의 방향 등을 이용한다. 그리고 이 같은 정보들을 종합적으로 분석하기 위한 연필과 종이 같은 계산 수단만 갖추면 된다. 선장은 자기 배가 이동한 만큼 선으로 그려나가면 된다. 어떤 때는 길게, 어떤 때는 짧게 종이에 표시하면 되는 것이다. 하지만 이는 길이만 잴 수 있다.

지금은 인공지능이 높은 수준으로 발전했으므로, 아마 대부분의 인간은 상대방이 인공지능임을 깨닫지 못하리라고 여길 것이다. 하지만 현재 기술로도 인공지능이 모든 문제를 쉽게 맞히기는 매우 어렵다. 예를 들어, 상대방에게 개 그림과 고양이 그림을 보여주면서 "어느 것이 개냐?"고 물어본다면 5살짜리 아이도 쉽게 대답할 수 있지만, 인공지능은 이러한 질문에 쉽게 답을 내리지 못한다. 특히, 그 개의 꼬리와 같은 일부분만 보여주거나 배경화면이 비슷한 상황에서 호랑이와 같이 있다면 인공지능은 혼란에 빠진다. 아직도 인공지능은 다양한 패턴에 대한 학습이 덜 되어있기 때문이다. 이러한 방식을 CAPTCHA(Completely Automated Public Turing test to tell Computers and Humans Apart)라고 하는데, 변형된 글자나 숨은그림 찾기 등 인지된 그림에서 특징을 찾아내는 과정에서 인간이 인공지능보다 더 우월하다는 것을 보여준다. 특히, 감정.억양.표정 등을 보여주었을 때 인공지능이 이를 구분하는 것은 더욱 어렵다.

사실 인간도 태어나면서부터 천성적으로 모든 사물을 인식하는 것은 아니다. 인식도 태어날 때부터 눈으로 보고 느낀 것을 계속 학습했기 때문에 가능하다. 예를 들어, 한 인간이 태어났을 때부터 평생 시각장애인으로 살아왔다가 수술로 시력을 찾은 경우를 보자. 그는 영화에서처럼 눈을 뜨자마자 부모님을 부둥켜안고 기뻐했을까? 하지만 그에게 가장 먼저 보인 것은 '뭐라 설명할 수 없는' 추상적인 그림과 같은 형태였다. 뇌가 학습하지 못했기에 형태·거리·색깔 등을 인식하지 못한 것이다. 결국 그는 형태·거리·색깔 등을 학습할 동안 다시 눈을 가리고 생활하는 것이 더 익숙하다는 사실을 알게 되었다.

이렇듯 인간도 태어날 때부터 자기 눈에 보이는 것에 대해 끊임없이 식별·파악·저장·회상하면서 자기 것으로 만든다. 어린아이가 아무것도 모르는 것 같은가? 하지만 누운 채 끊임없이 사물을 학습하고, 기억을 저장하는 중이다.

폰 노이만과 앨런 튜링, 이 두 인간을 바라보노라면 "결국 인공지능과 사이버보안은 공통점을 가지고 있다"는 사실을 알 수 있다. 그들은 IT 전문가이면서 인공지능·사이버보안 전문가였다. 인공지능의 수준을 높이려면 사이버보안 관련 지식과 경험이 있어야 하며, 사이버보안 문제를 해결하면 자연스레 인공지능 관련 기술의 과제도 쉽게 풀 수 있다. 결국, 인공지능과 사이버보안은 도저히 뗄 수 없는 관계, 즉 물과 물고기의 관계를 맺고 있다. 물고기는 물이 없으면 죽을 것이고, 물에 물고기가 없으면 의미가 없다는 수어지교(水魚之交)의 교훈에 따라 인공지능 분야와 사이버보안 분야가 함께 갈 수 있도록 정책과 인식을 마련해야 할 것이다.

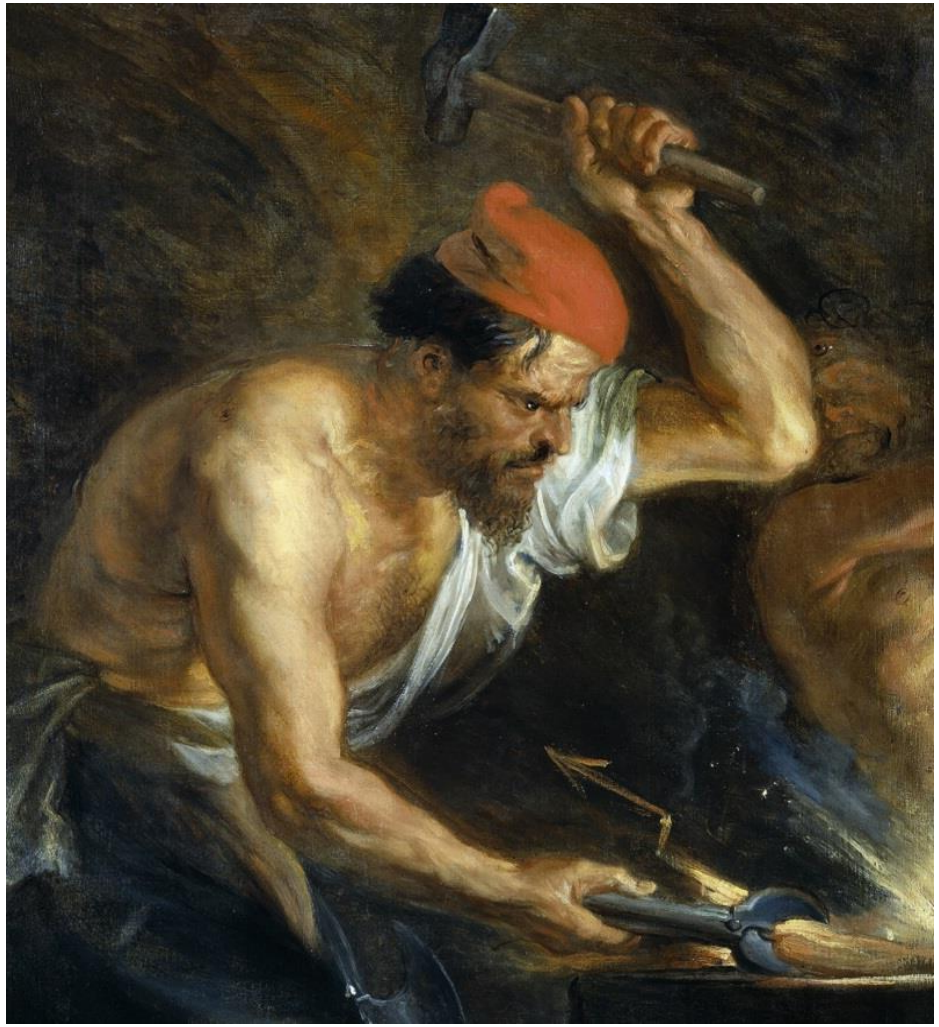
[글_ 김주원 사이버보안 분야 칼럼리스트]

1 AI vs 사이버보안

인공지능(AI) = 사이버

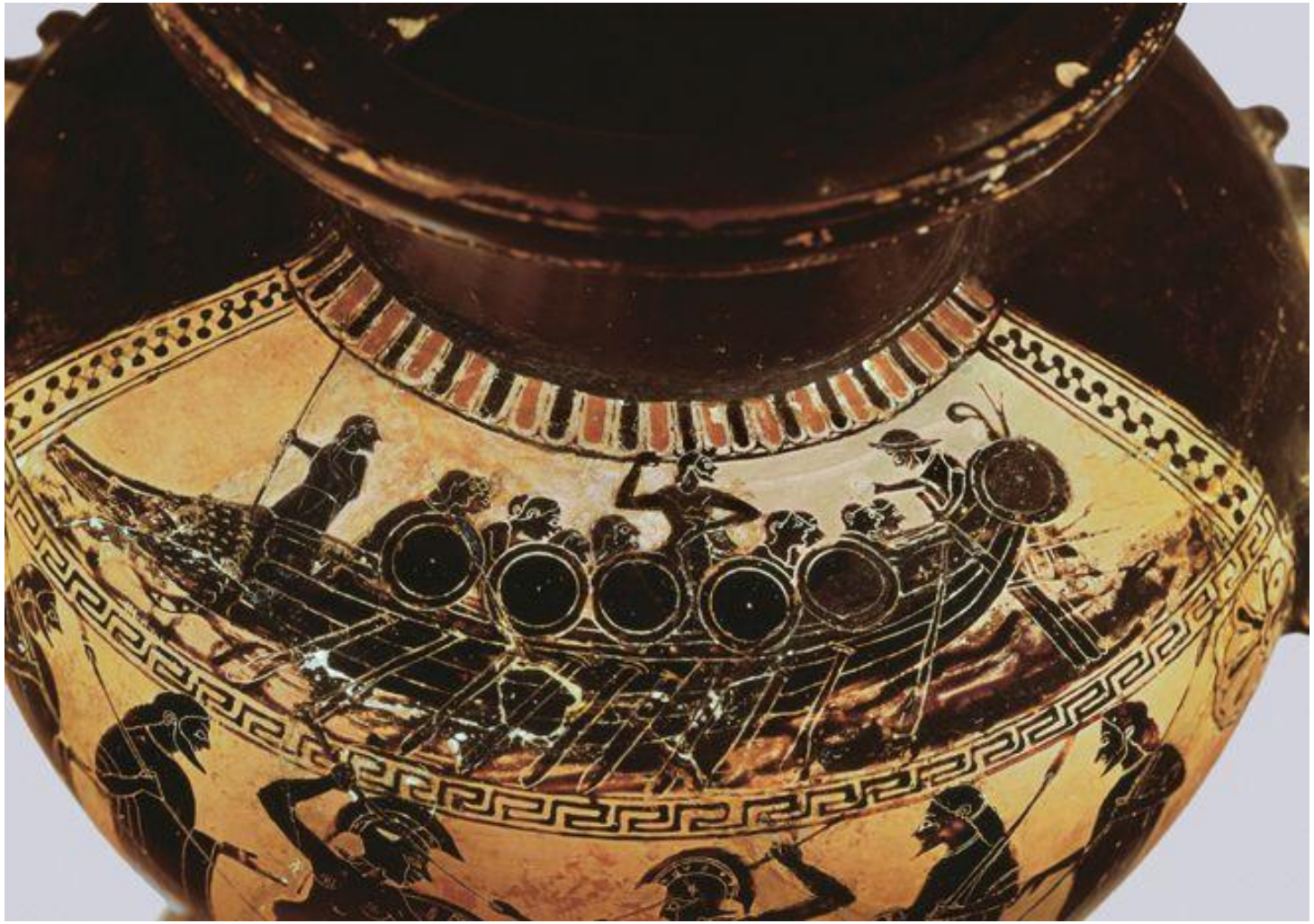
그리스 신화를 보면 인공지능 관련 내용이 다수 포함

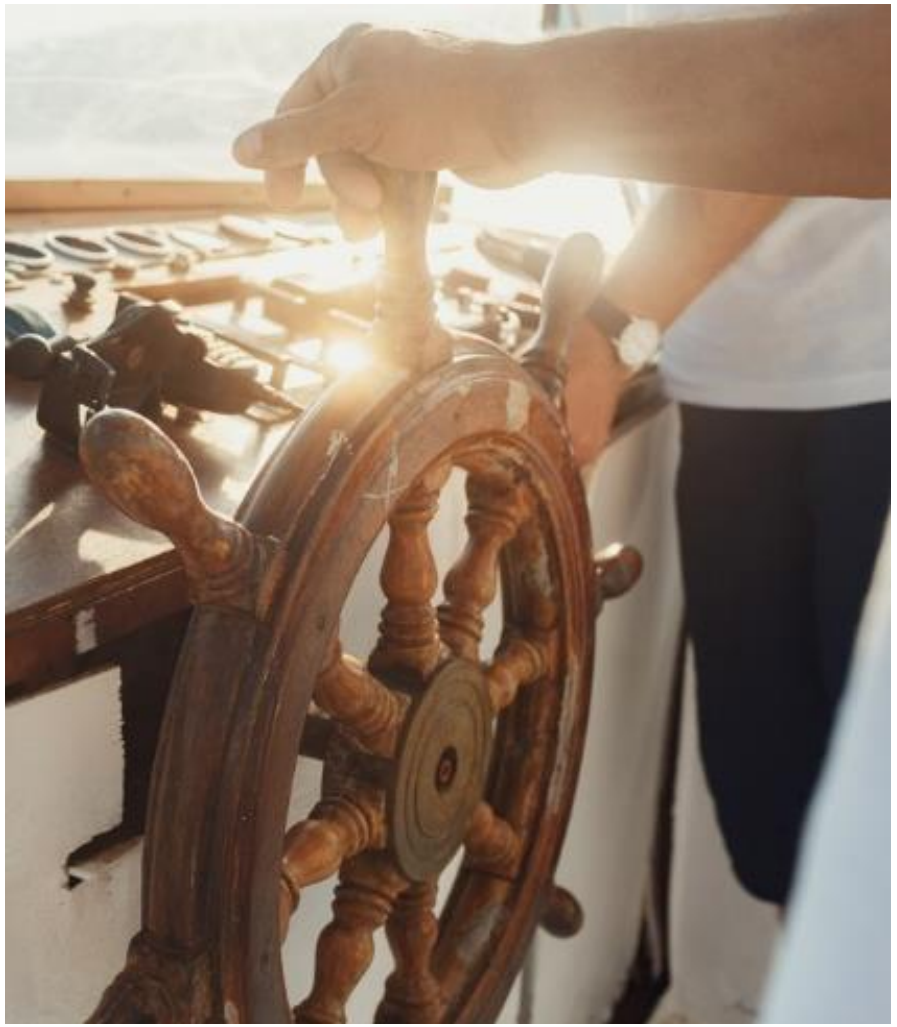
헤파이스토스 : 대장장이 신



인공지능 로봇, 드론, 무인이동체, 빅데이터 등 다수의 기기 개발 및 제작

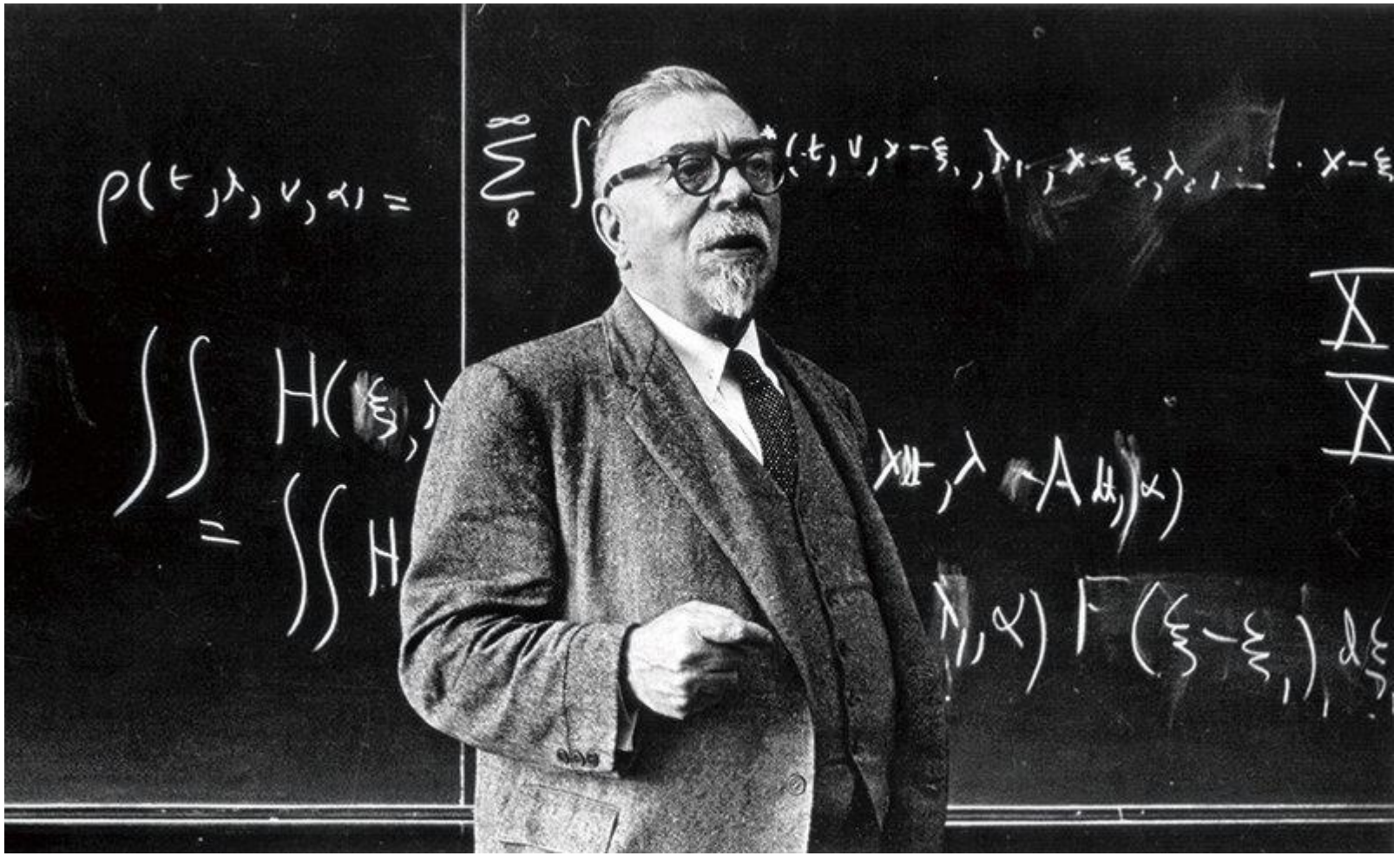
퀴베르네테스(Kybernetes) : 키잡이, Cyber의 어원



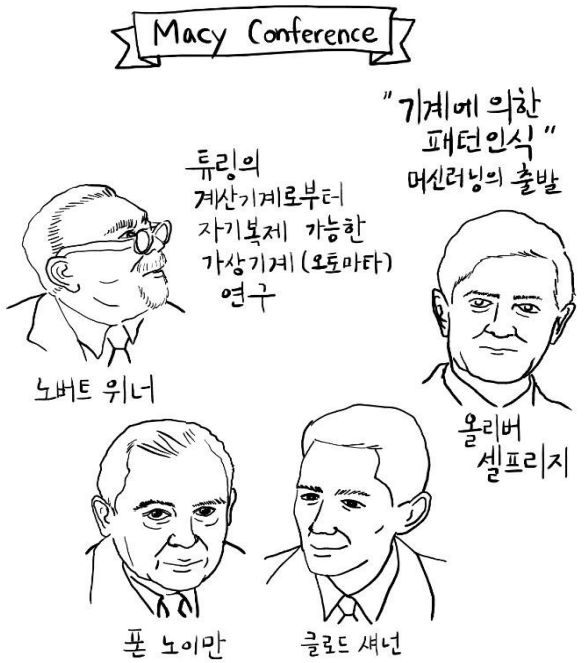


여인의 머리 속에서 나온 저장 장치 : 빅데이터, 인공지능(AI)의 운영체제

사이버네틱스 : 인공두뇌학

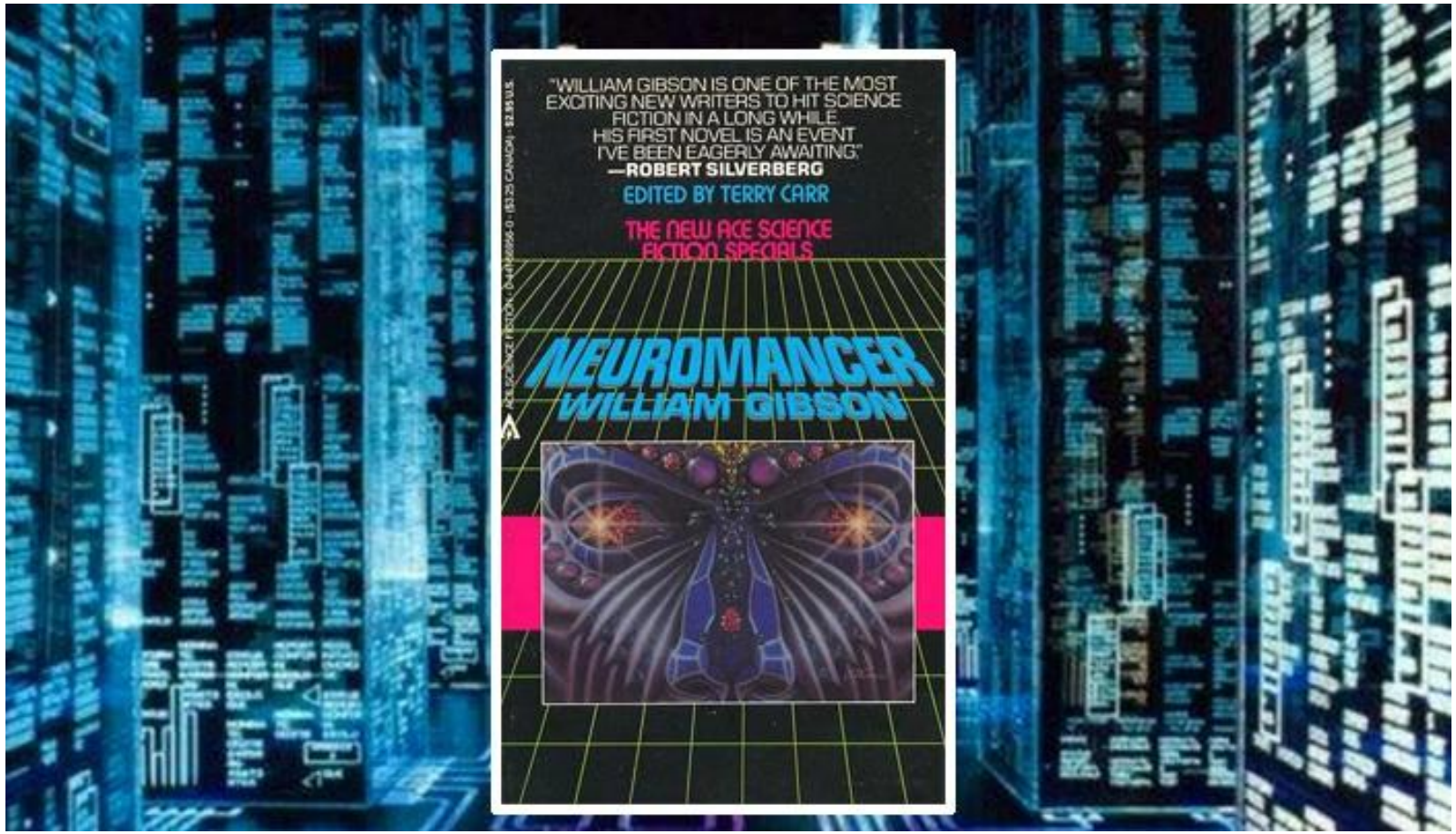


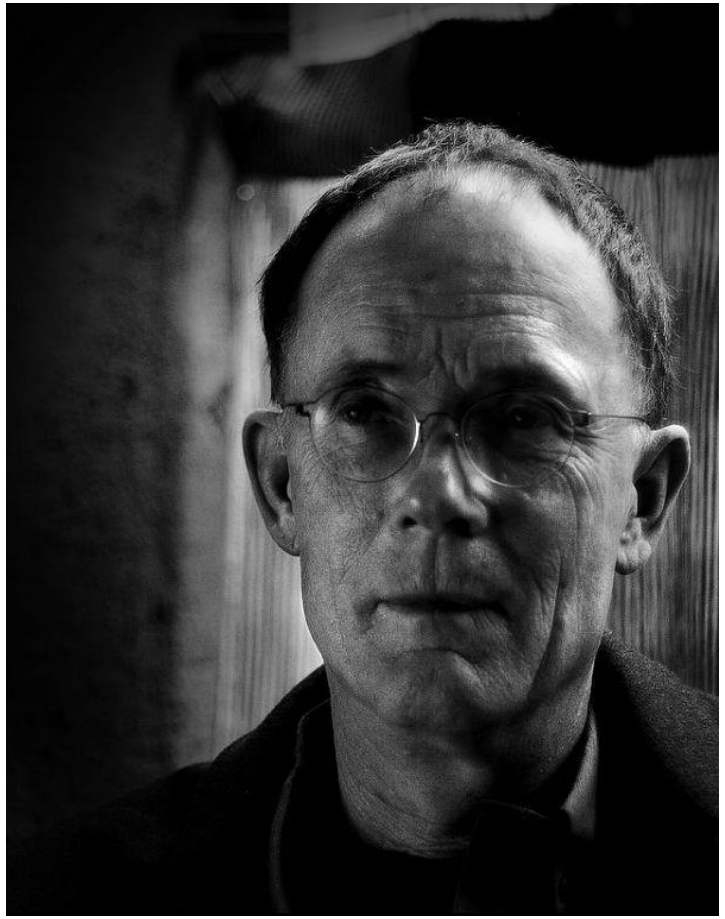
세계 제2차대전이 끝나고
노버트 위너를 중심으로 모인
사이버네틱스 그룹은 '메이시 학회'를
조직해서 자신들의 새로운 이론을
세상에 퍼뜨립니다.



로버트 위너 교수(1948) : '동물과 기계가 상호 작용하는 방법' 에서 처음 제안

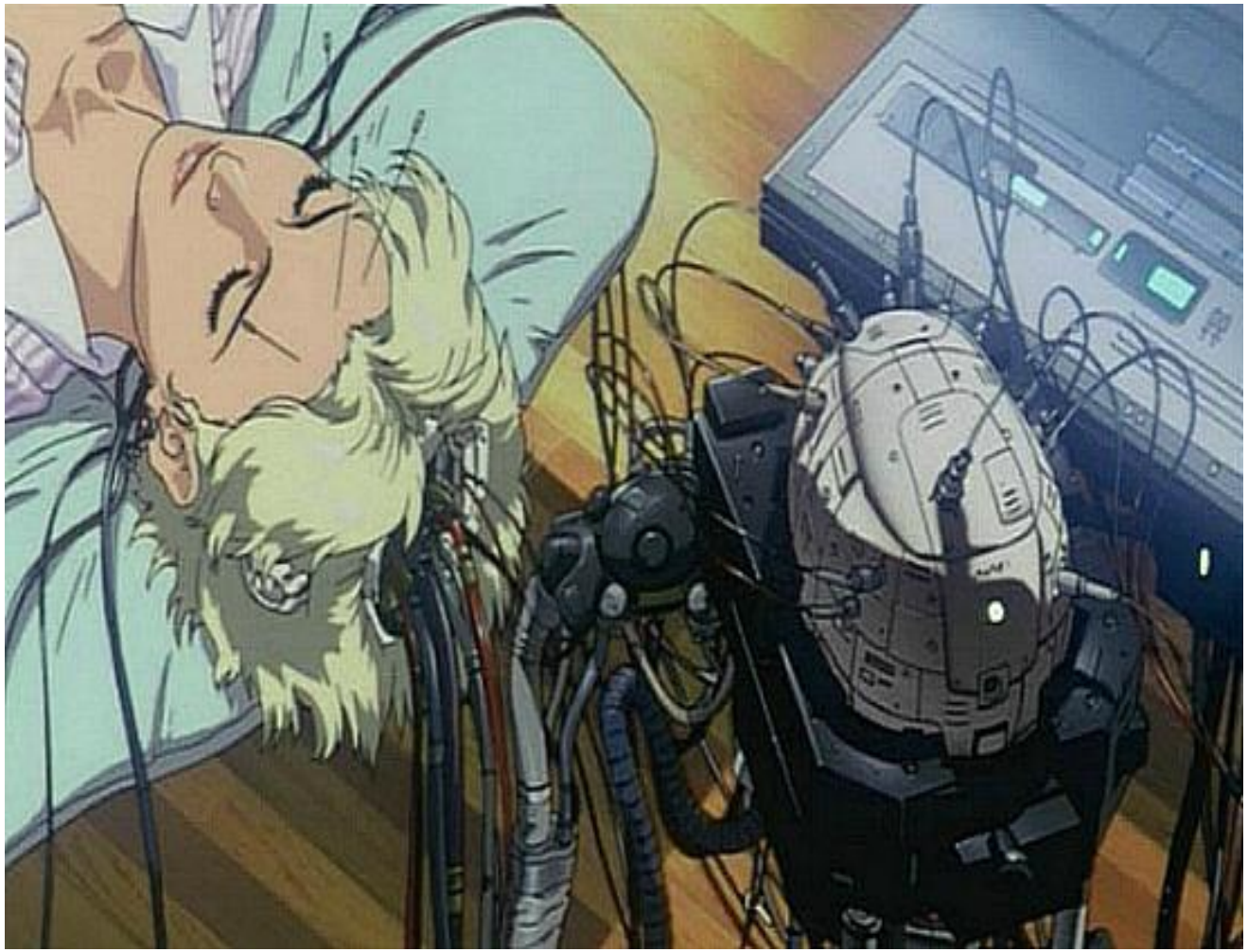
사이버보안의 어원 : Neuromancer





미국의 SF 작가 윌리엄 깁슨이 사이버 공간, 사이버 보안을 첫 언급

인공지능과 사이버전사, 해킹, 바이러스

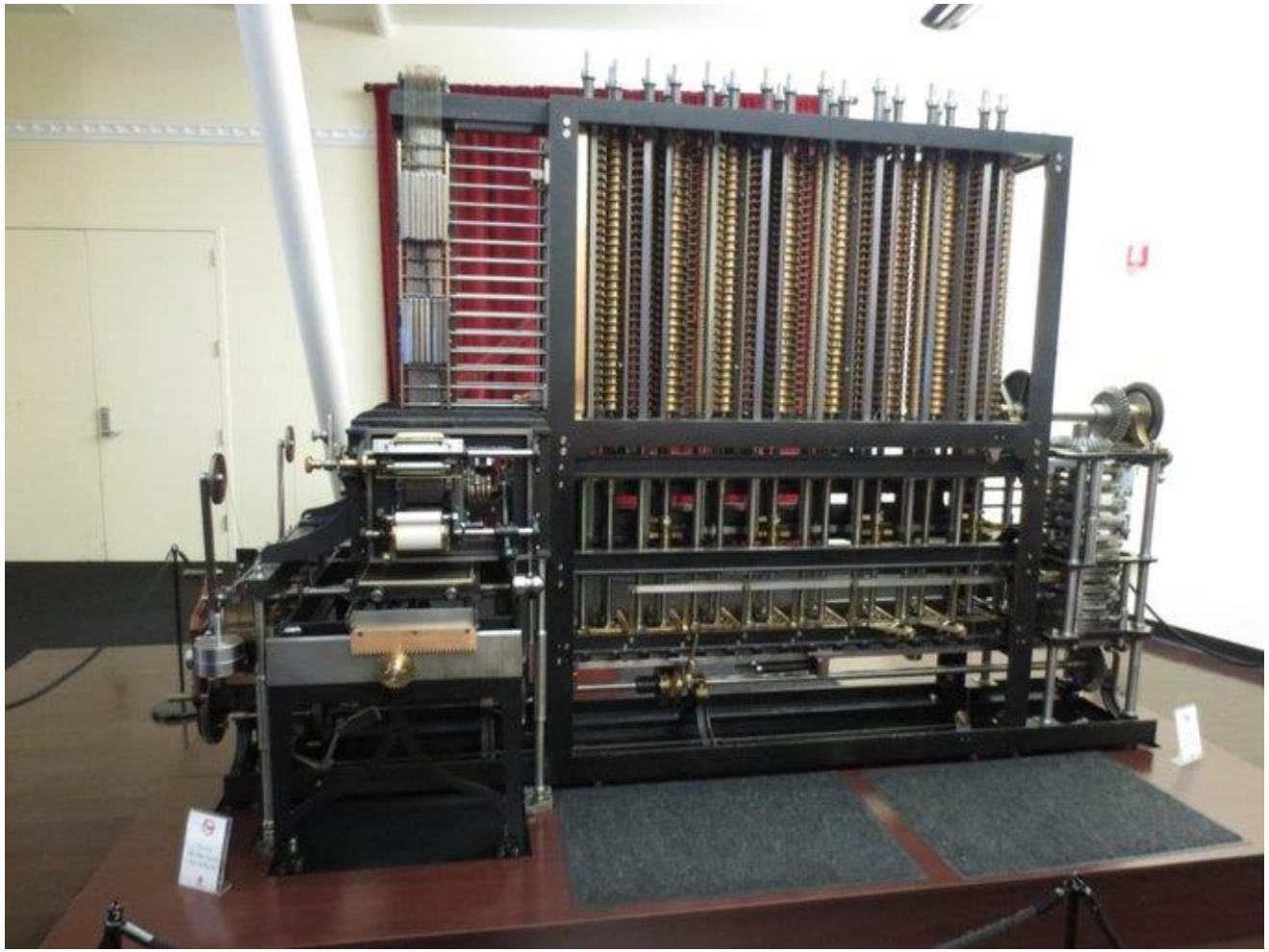


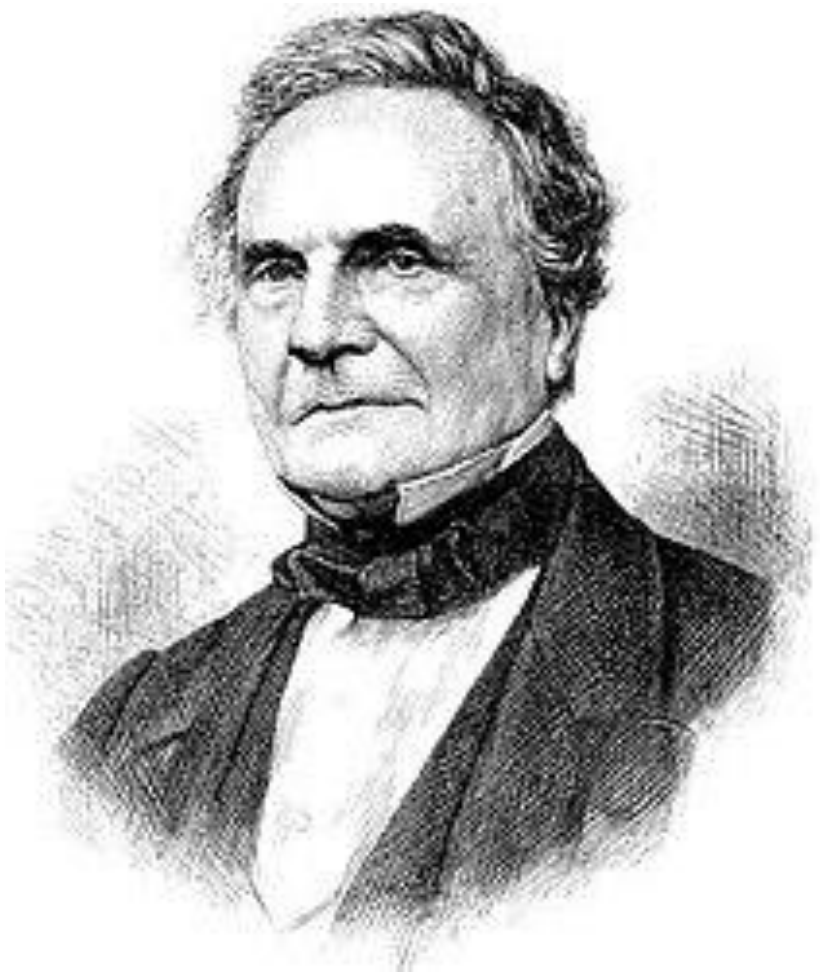
공각기동대, 매트릭스 등 SF 영화에서 상호 경쟁으로 표현

안티키테라 기계(Antikythera Mechanism)

기원전 100년경에 만들어진 아날로그 컴퓨터 : 천문 및 선박 항해 계산

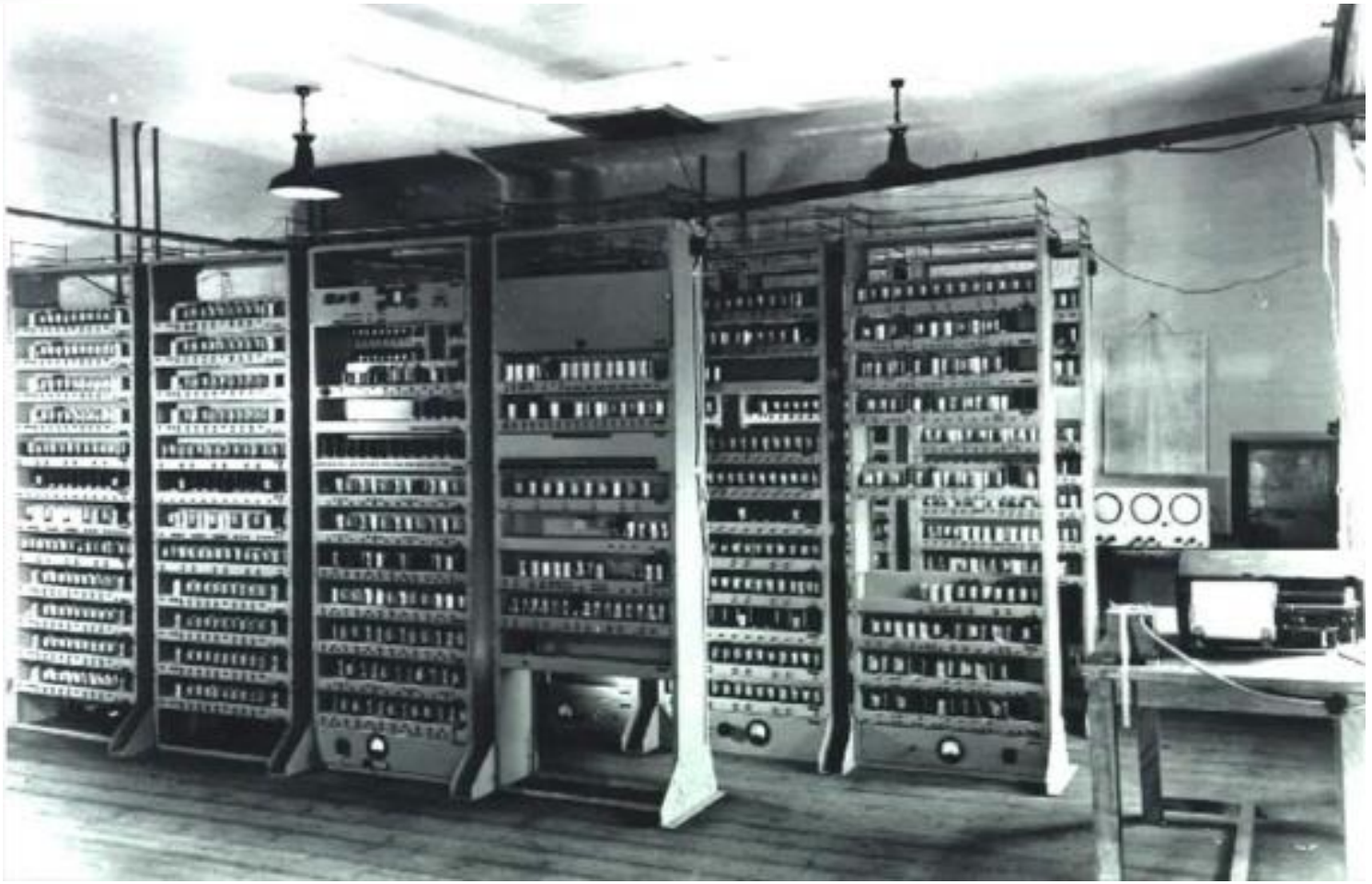
찰스 배비지의 차분 기관 (Difference Engine)





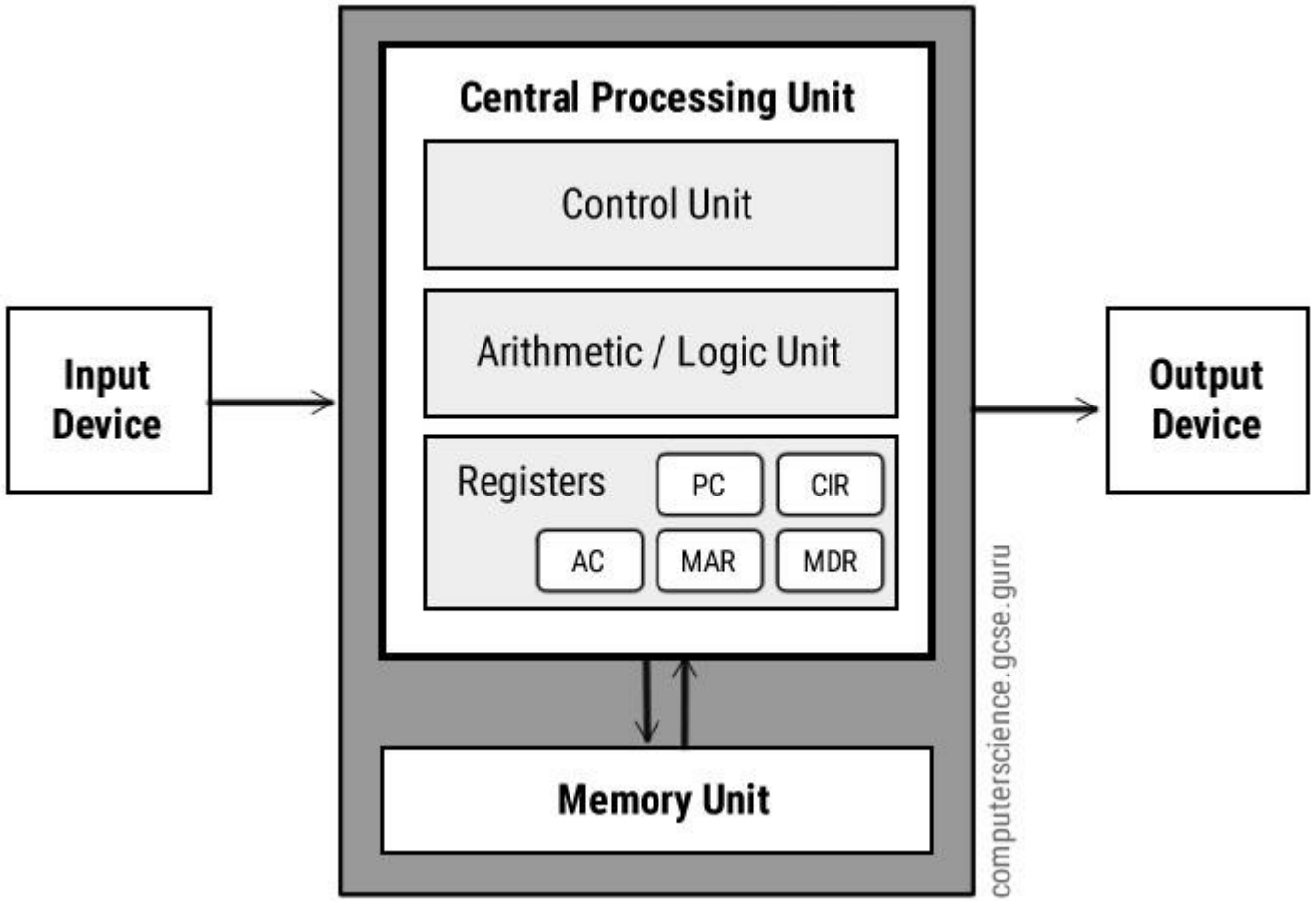
로그함수와 삼각함수 계산 : 인쇄기에 적용(도서의 대량생산 및 보급)

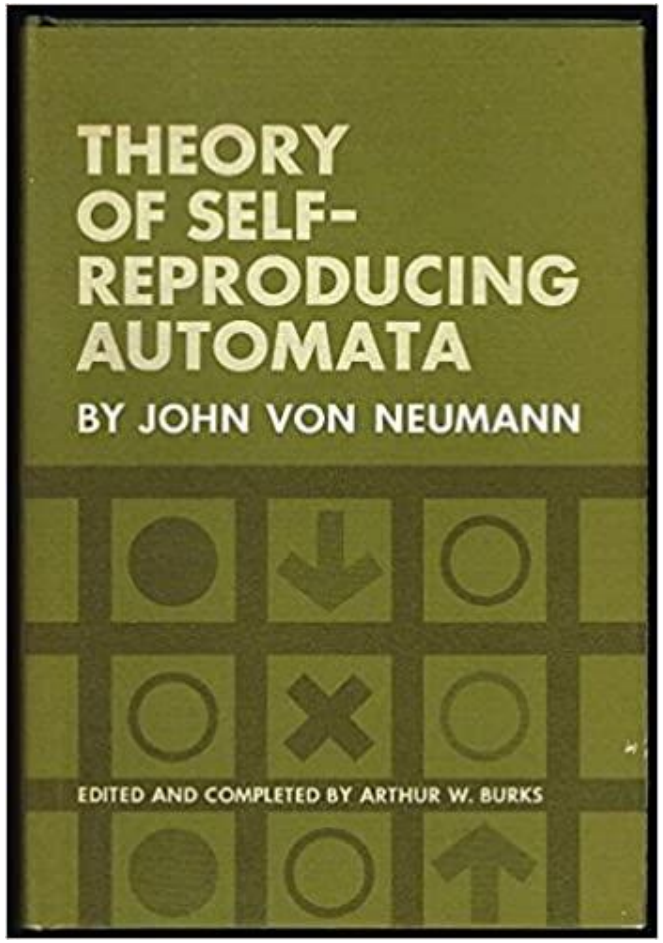
폰 노이만과 컴퓨터



2차 세계대전에 사용된 무기에 대한 모델링, 시뮬레이션에 적용

폰 노이만 : 자신의 컴퓨터에 취약점 발견





1949년 “theory and organization of complicated automata” 에서
자기 복제를 통해 스스로 증식할 수 있다는 가능성 제시

폰 노이만 : 인간의 뇌 구조를 인공으로 만들 수 있다.

Artificial Intelligence and Neural Networks The Legacy of Alan Turing and John von Neumann

Heinz Muehlenbein
Fraunhofer Institut Autonomous intelligent Systems
Schloss Birlinghoven 53757 Sankt Augustin, Germany
heinz.muehlenbein@online.de, http://www.ais.fraunhofer.de/~muehlen

***Abstract*— The work of Alan Turing and John von Neumann on machine intelligence and artificial automata is reviewed. Turing's proposal to create a child machine with the ability to learn is discussed. Von Neumann's had doubts that with teacher based learning it will be possible to create artificial intelligence. He concentrated his research on the issue of complication, probabilistic logic, and self-reproducing automata. The problem of creating artificial intelligence is far from being solved. In the last sections of the paper I review the state of the art in probabilistic logic, complexity research, and transfer learning. These topics have been identified as essential components of artificial intelligence by Turing and von Neumann.**

I. Introduction

Computer based research on machine intelligence started about 60 years ago, parallel to the construction of the first electronic computers. Therefore it seems to be time again to compare todays state-of-the art with thoughts and proposals at the very beginning of the computer age. I have chosen Alan Turing and John von Neumann as the most important representatives of the first concepts of machine intelligence. Both researchers actually designed electronic computers, but they also reflected about what the new electronic computers could be expected to solve in addition to numerical computation. Both discussed intensively the problem how the performance of the machines will ultimately compare to the power of the human brain.

In this paper I will first review the work of Alan Turing, contained in his seminal paper "Computing Machinery and Intelligence" (17) and in the not so well known paper "Intelligent Machinery" (18). Then I will discuss the most important paper of John von Neumann concerning our subject "The General and Logical Theory of Automata" (22). All three papers have been written before the first electronic computers became available. Turing even wrote programs for paper machines.

I will describe the thoughts and opinions of Turing and von Neumann in detail, without commenting them using todays knowledge. Then I will try to evaluate their proposals in answering the following questions

- What are their major ideas for creating machine intelligence?
- Did their proposals lack important components we see as necessary today?
- What are the major problems of their designs and do their exists solutions today?

This paper extends my research started in (12).

II. Turing and machine intelligence

The first sentences of the paper "Computing machinery and intelligence" have become famous. "I propose to consider the question "Can machines think?" This should begin with definitions of the meaning of the terms "machine" and "think"....But this is absurd. Instead of attempting such a definition I shall replace the question by another, which is closely related to it and is expressed in relatively unambiguous words. The new form of the question can be described in terms of a game which we call the imitation game."

The original definition of the imitation game is more complicated than what is today described as the Turing test. Therefore I describe it shortly. It is played with three actors, a man (A), a woman (B) and an interrogator (C). The object of the game for the interrogator is to determine which of the other two is the man and which is the woman. It is A's objective in the game to try and cause C to make the wrong identification. Turing then continues: "We now ask the question "What will happen when a machine takes the part of A in the game?" Will the interrogator decide wrongly as often when the game is played as this as he does when the game is played between a man and a woman? These questions will replace our original "Can machines think".

Why did Turing not define just a game between a human and a machine trying to imitate a human, as the Turing test is described today? Is there an additional trick in introducing gender into the game? There has been a quite a lot of discussions if this game characterizes human intelligence at all. Its purely behavioristic definition leaves out any attempt to identify important components which together produce human intelligence. I will not enter this discussion here, but just state the opinion of Turing about the outcome of the imitation game.
"It will simplify matters for the readers if I explain first my own beliefs in the matter. Consider first the more accurate form of the question. I believe that in about fifty years' time it will be possible to programme computers with a storage capacity of about 10^9 bits to make them play the imitation game so well that an average interrogator will not have more than 70% chance of making the right identification after five minutes of questioning."
The accurate form of the question is obviously artificial definite: Why a 70% chance, how often has the game to be played, why a duration of five minutes? In the next section I will discuss what Turing lead to predict 50 years. The prediction is derived in section 7 of his paper, where Turing discusses learning machines (17).

III. Turing's construction of an intelligent machine

In section 7 Turing discusses the construction of an intelligent machine. In the sections before Turing mainly refuses general philosophical arguments against intelligent machines. "The reader will have anticipated that I have no very convincing argument of a positive nature to support my views. If I had I should not have taken such pains to point out the fallacies in contrary views. Such evidence as I have I shall now give." What is Turing's evidence?

"As I have explained, the problem is mainly one of programming. Advances in engineering will have to be made too, but it seems unlikely that these will not be adequate for the requirements. Estimates of the storage capacity of the brain vary from 10^{10} to 10^{15} binary digits.[1] I incline to the lower values and believe that only a small fraction is used for the higher types of thinking. Most of it is probably used for the retention of visual impressions. I should be surprised if more than 10^9 was required for satisfactory playing of the imitation game. Our problem then is to find out how to programme these machines to play the game. At my present rate of working I produce about a thousand digits of programme a day, so that about sixty workers, working steadily through fifty years might accomplish the job, if nothing went into the wastepaper basket."

The time to construct a machine which passes the imitation game is derived from an estimate of the storage capacity of the brain [2] and the speed of programming. Turing did not see any problems in creating machine intelligence purely by programming, he just found it too time consuming. So he investigated if there exist more expeditious methods. He observed. "In the process of trying to imitate an adult human mind we are bound to think a good deal about the process which has brought it to the state that it is in. We may notice three components.

1) The initial state of the brain, say at birth.
2) The education to which it has been subjected.
3) Other experience, not to be described as education, to which it has been subjected.

Instead of trying to produce a programme to simulate an adult mind, why not rather try to produce one which simulates the child's...Presumably the child brain is something like a notebook. Rather little mechanism, and lots of blank sheets. Our hope is that there is so little mechanism in the child brain that something like it can easily be programmed. The amount of work in the education we can assume, as a first approximation, to be much the same as for the human child."

A. Turing on learning and evolution

In order to achieve a greater efficiency in constructing a machine with human like intelligence, Turing divided the problem into two parts

- The construction of a child brain
- The development of effective learning methods

Turing notes that the two parts remain very closely related. He proposes to use experiments: teaching a child machine and see how well it learns. One should then try another and see if it is better or worse. "There is an obvious connection between this process and evolution, by the identifications

- structure of the machine = hereditary material
- changes of the machine = mutations
- Natural selection = judgment of the experimenter

Survival of the fittest is a slow process of measuring advantages. The experimenter, by the exercise of intelligence, should be able to speed it up."

Turing then discusses learning methods. He notes ((17),p.454):"We normally associate the use of punishments and rewards with the teaching process...The machine has to be so constructed that events which shortly proceeded the occurrence of a punishment signal are unlikely to be repeated, whereas a reward signal increased the probability of repetition of the events which lead to it." But Turing observes the major drawback of this method:"The use of punishments and rewards can at best be part of the teaching process. Roughly speaking, if the teacher has no other means of communicating to the people, the amount of information which can reach him does not exceed the total number of rewards and punishments applied."
In order to speed up learning Turing demanded that the child machine should understand some language. In the final pages of the paper Turing discusses the problem of the complexity the child machine should have. He proposes to try two alternatives: either to make it as simple as possible to allow learning or to include a complete system of logical inference. He ends his paper with the remarks: "Again I do not know the answer, but I think both approaches should be tried. We can see only see a short distance ahead, but we can see plenty there that needs to be done."

B. Turing and neural networks

In the posthumously published paper *Intelligent Machinery* (18) Turing describes additional details how to create an intelligent machine. First he discusses possible components of a child machine. He introduces *unorganized machines* of type A,B, and P. A and B are artificial neural networks with random connections. They are made up from a rather large number N of similar units, which can be seen as binary neurons. Each unit has two input terminals and one output terminal which can be connected to the input terminals of 0 (or more) other units. The connections are chosen at random. All units are connected to a central synchronizing unit from which synchronizing pulses are emitted. Each unit has two states. The dynamics is defined by the following rule:

The states from the units from which the input comes are taken from the previous moment, multiplied together and the result is subtracted from 1.

This rule gives the following transition table.

0	0	1
1	0	1
0	1	1
1	1	0

The state of the network is defined by the states of the units. Note that the network might have lots of loops, it continually goes through a number of states until a period begins. The period cannot exceed 2^N cycles. In order to allow learning the machine is connected with some input device which can alter its behavior. This might be a dramatic change of the structure, or changing the state of the network. Maybe Turing had the intuitive feeling that the basic transition of the type A machine is not enough, therefore he introduced the more complex B-type machine. I will not describe this machine here, because neither for the A or the B machine Turing defined precisely how learning can be done.
A learning mechanism is introduced with the third machine, called a P-type machine. The machine is an automaton with a number of N configurations. There exist a table where for each configuration is specified which action the machine has to take. The action may be either

1) To do some externally visible act $A_1, \ldots A_k$
2) To set a memory unit M_i

The reader should have noticed that the next configuration is not yet specified. Turing surprisingly defines: The next configuration is always the remainder of $2s$ or $2s+1$ on division by N. These are called the alternatives 0 and 1. The reason for this definition is the learning mechanism Turing defines. At the start the description of the machine is largely incomplete. The entries for each configuration might be in five states, either U (uncertain), or T0 (try alternative 0), T1 (try alternative 1), D0 (definite 0) or D1 (definite 1).

Learning changes the entries as follows: If the entry is U, the alternative is chosen at random, and the entry is changed to either T0 or T1 according to whether 0 or 1 was chosen. For the other four states, the corresponding alternatives are chosen. When a pleasure stimulus occurs, state T is changed to state D, when a pain stimulus occurs, T is changed to U. Note that state D cannot be changed. The proposed learning method sounds very simple, but Turing surprisingly remarked:

I have succeeded in organizing such a (paper) machine into a universal machine.

Today this universal machine is called the Turing Machine. Turing even gave some details of this particular P-type machine. Each instruction consisted of 128 digits, forming four sets of 32 digits, each of which describes one place in the main memory. These places may be called P,Q,R,S. The meaning of the instruction is that if p is the digit at P and q that at Q then $1 - pq$ is to be transferred to position R and the next instruction will be found at S. The universal machine is not the solution to the problem, it has to be programmed!

C. Discipline and initiative

We now turn to the next important observation of Turing. Turing notes that punishment and reward are very slow learning techniques. So he requires:

If the untrained infant's mind is to become an intelligent one, it must acquire both discipline and initiative.

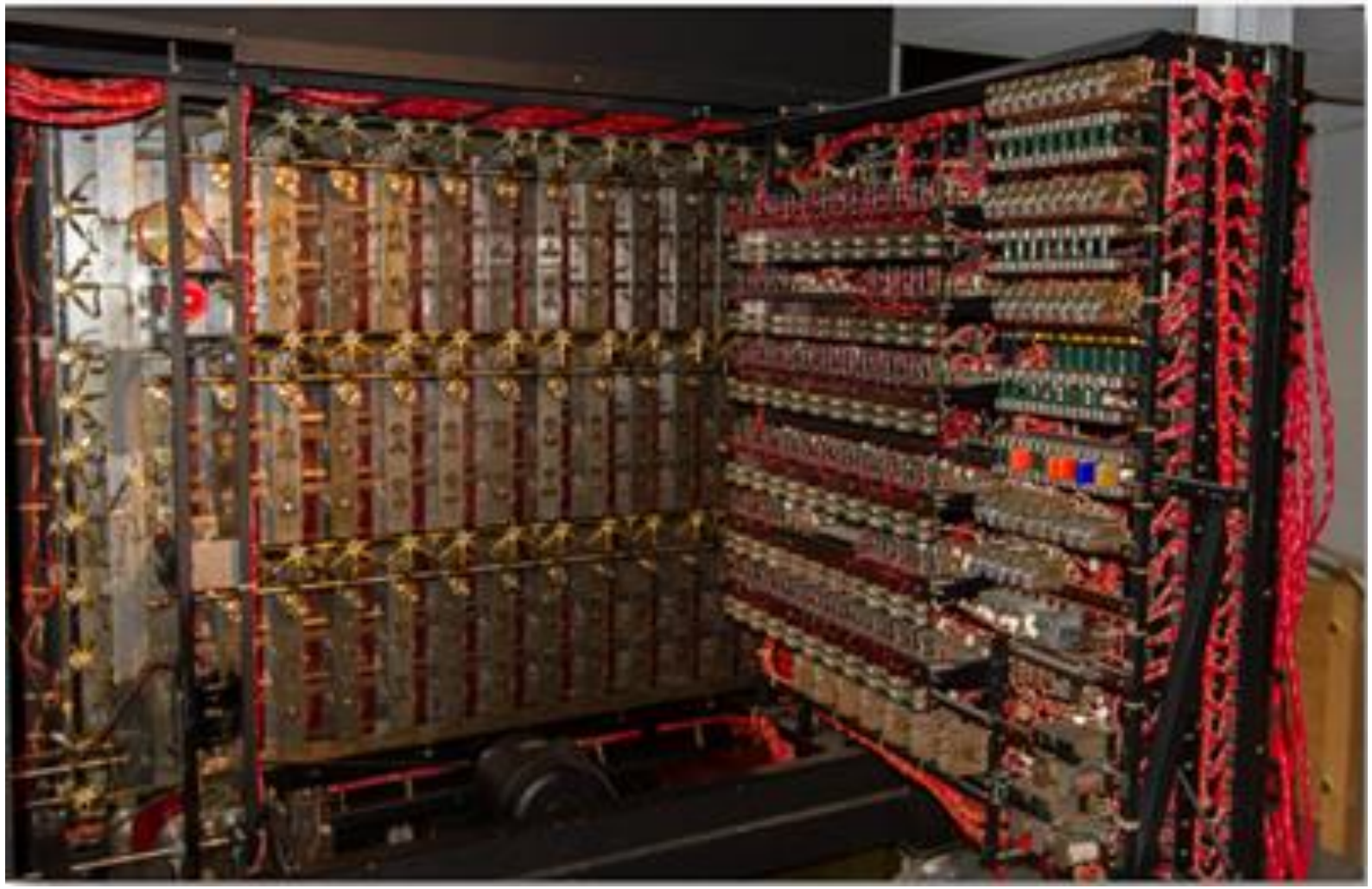
Discipline means strictly obeying the punishment and reward. But what is initiative? The definition of initiative

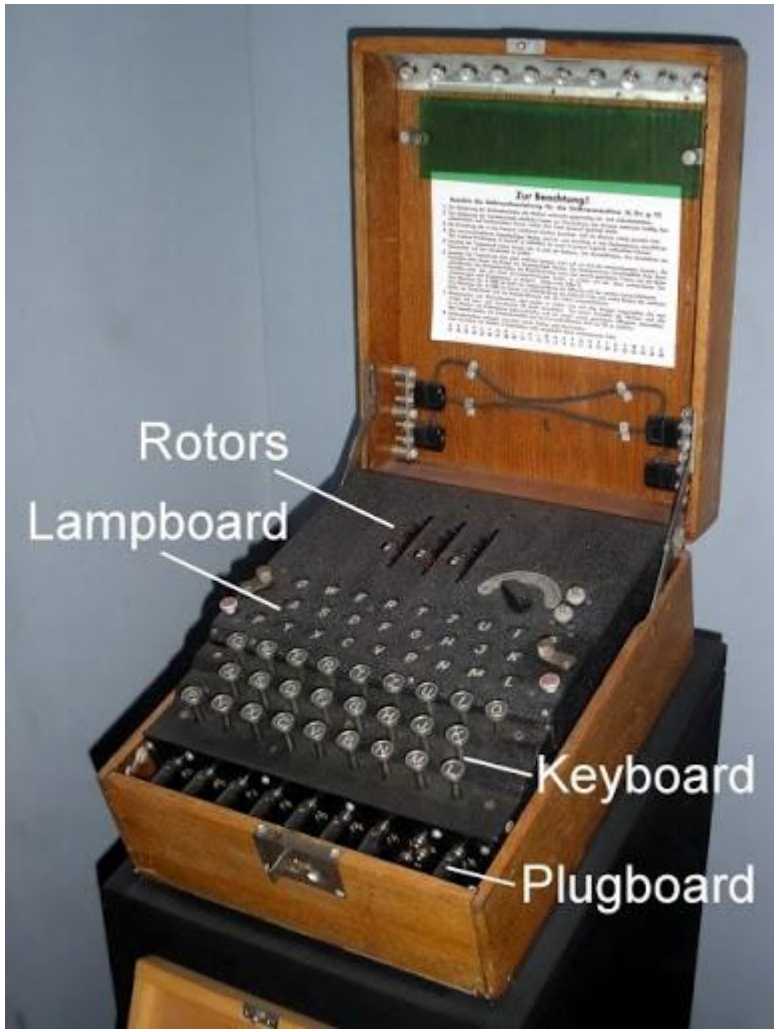
[1] At this time the number of neurons was estimated as being between 10^{10} to 10^{15}. This agrees with the estimates using todays knowledge.

[2] It was of course a big mistake to set the storage capacity equal to the number of neurons! We will later show that von Neumann estimated the storage capacity of the brain to be about 10^{20}.

이후, 인공지능에 대한 연구 수행

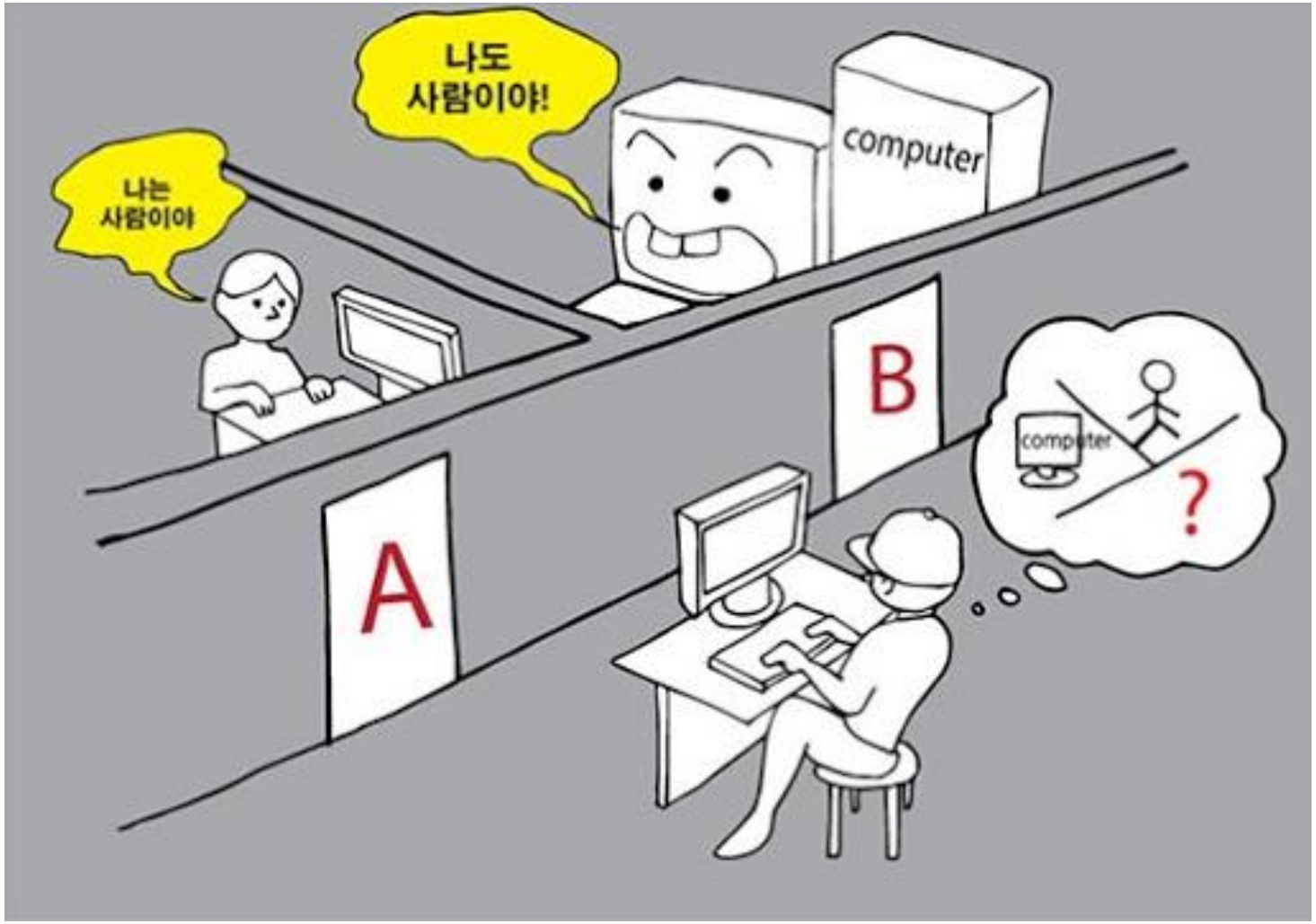
앨런 튜링 : 애니그마 해독





2차 세계 대전, 독일군의 암호 체계를 컴퓨터로 해독

앨런 튜링 : 인공지능과 이미테이션 게임(튜링 테스트)



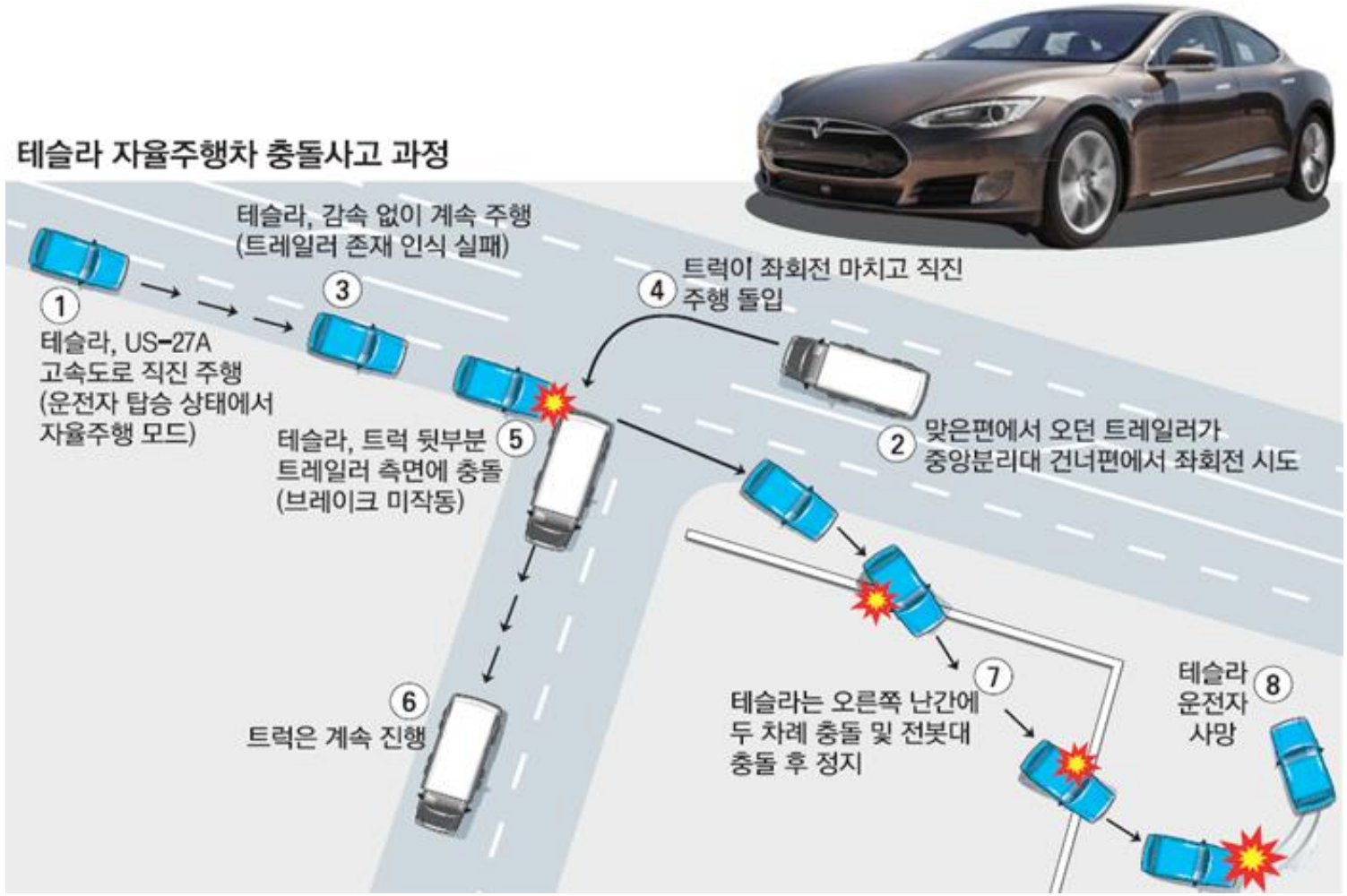
1950년 “컴퓨터와 지능 " 에서 튜링 테스트 제시

인공지능과 사이버는 출발점 = 추구하는 목표가 같다

인공지능을 이해하기 위해서는 경쟁이 아닌 사이버의 의미를 같이 이해해야 한다.

2 AI의 사이버 위협

자율주행 자동차의 판단착오

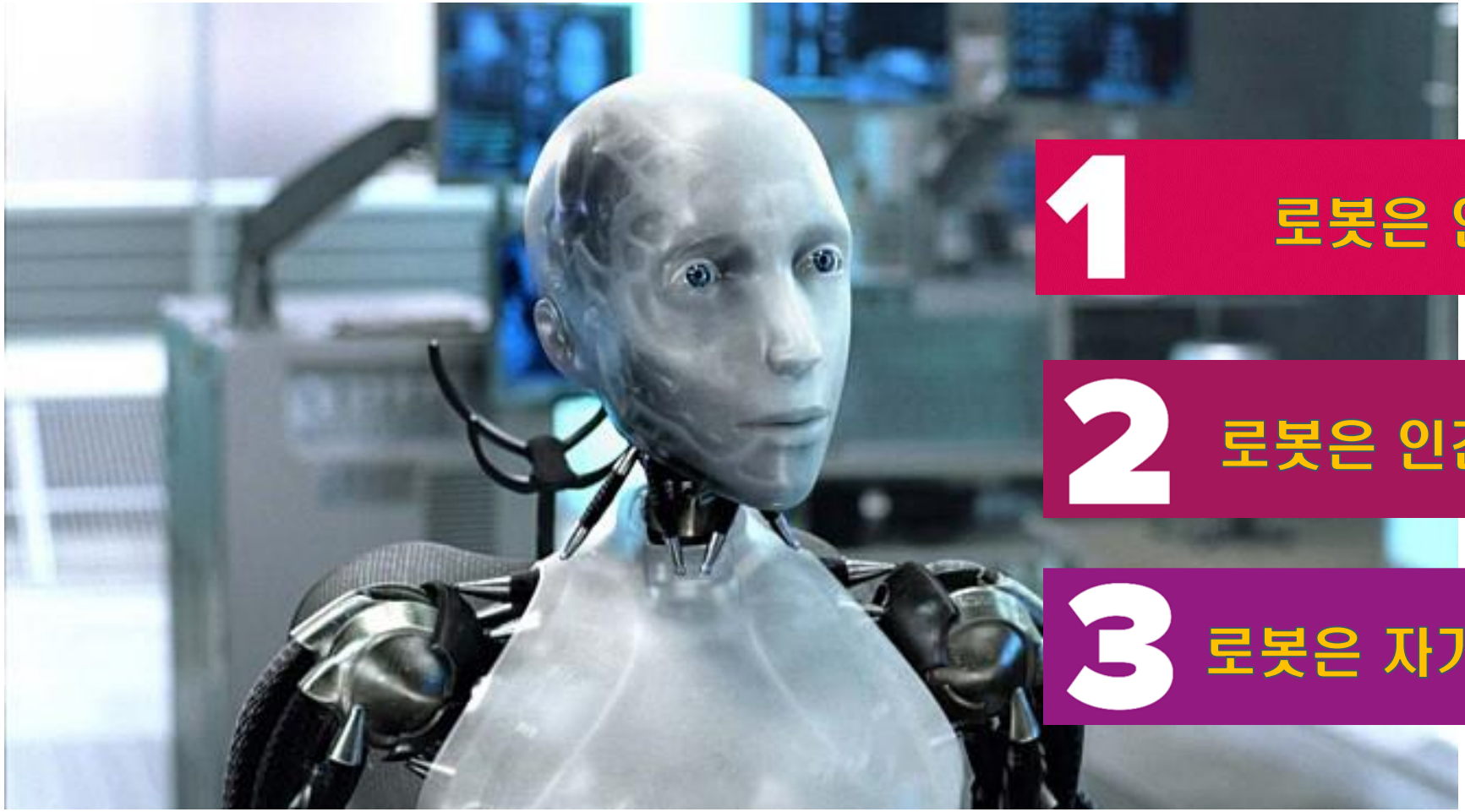


센서만으로는 한계 드러나, 사망사고 발생 (2016년, 2018년)

무인기의 민간인 폭격

군인과 민간인을 분리 식별 미흡, 부정확한 목표 지점 선정 등 (2013년)

로봇의 3원칙 – 아이작 아시모프



1 로봇은 인간을 지켜야 한다.

2 로봇은 인간의 명령을 들어야 한다.

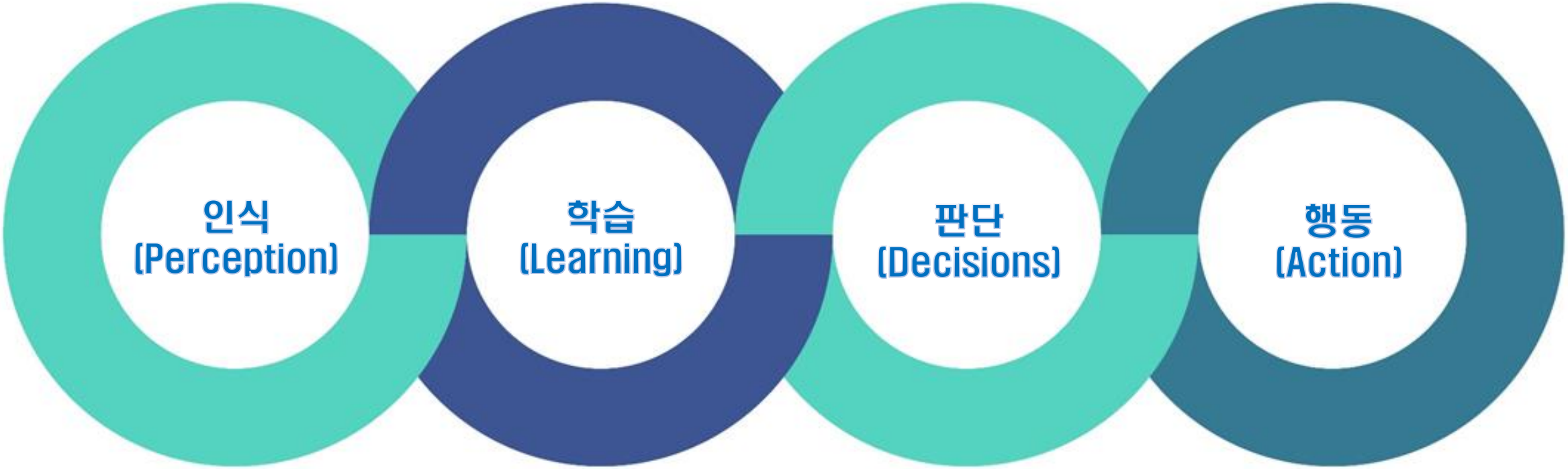
3 로봇은 자기 스스로도 지켜야 한다.

(질문) 혹시 프로그램 개발하실 때, 이 원칙을 반영하신 분 계신가요?

증시 폭락

뜬금없는 뉴욕증시 폭락, 알고보니 증권사 AI가 동시 투매 (2018년)

인공지능의 세부 프로세스



비정상적인 입력만 가지고서도 인공지능 시스템을 무력화 가능

보안에 강한 학습방법을 모색할 필요가 있음

빅데이터 시대

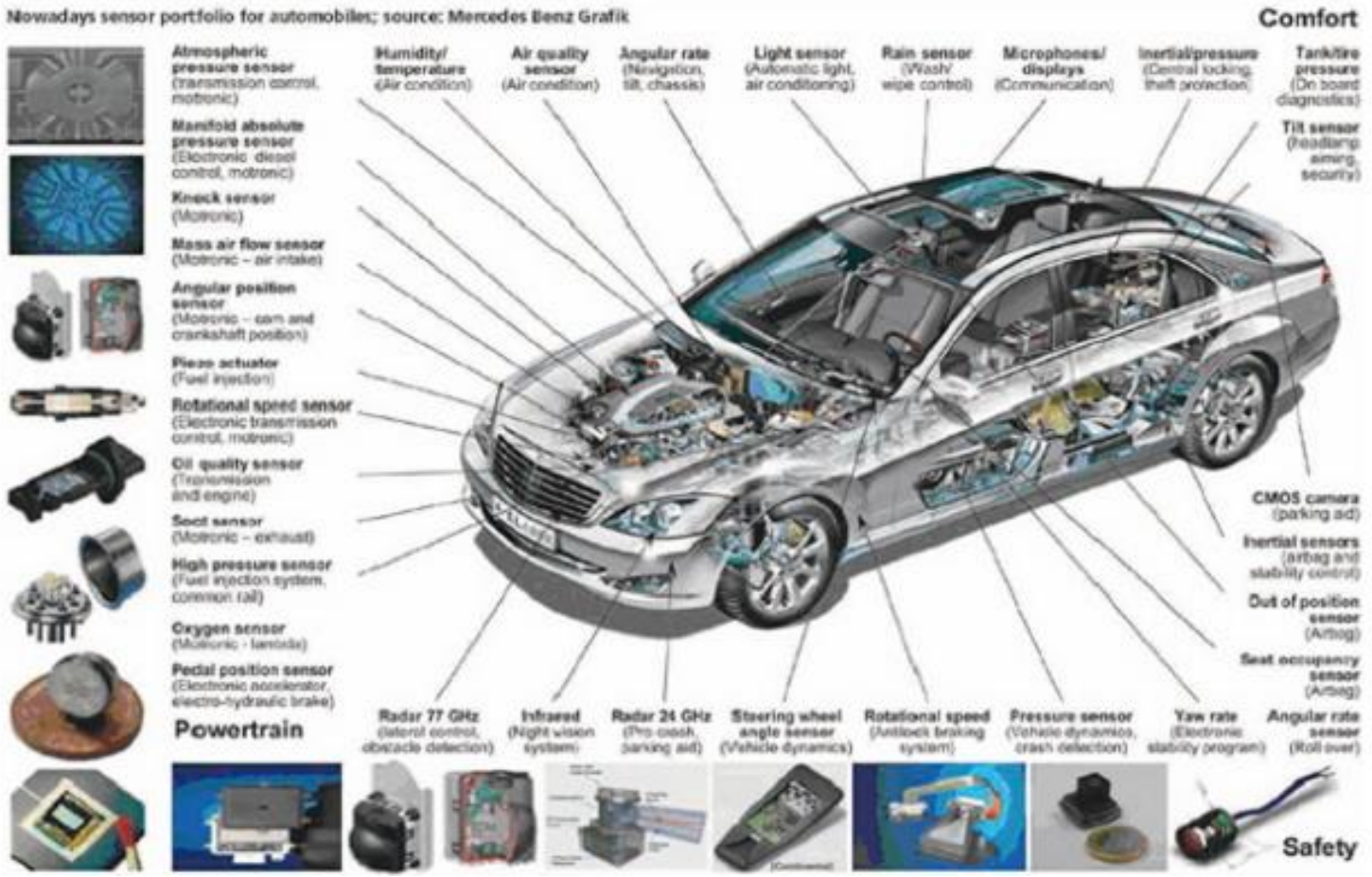
인공지능 학습을 위하여 빅 데이터 수집, 처리는 필수

인공지능의 학습용 데이터 셋 명확화

진눈깨비, 우박, 폭설 등 다양한 환경 변화에 맞추어 반응 결과도 다름

지진, 소용돌이와 같은 경험하지 못한 부분에 대한 데이터 구축 필요

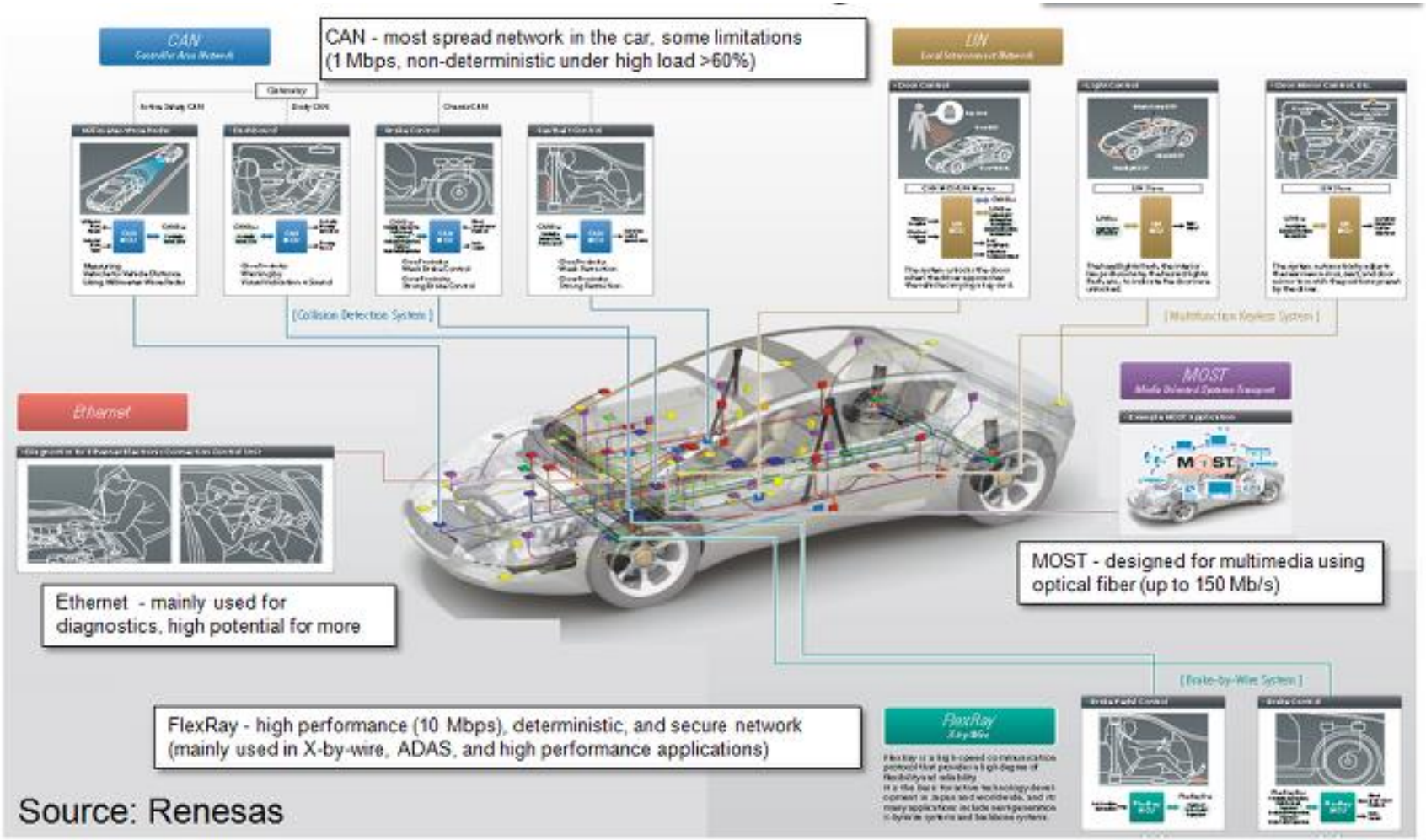
인공지능 소자/센서의 장애



자동차에 들어가는 부품만 해도 2만개가 넘는 상황에서 하나의 센서가

고장 또는 오 동작 하더라도 이를 감내할 수 있도록 설계

인공지능의 통신 에러



인간, 자동차, 고속도로 등 각종 주변 기기들과 연동하고, 통신을 하는 과정에서

통신 에러가 발생하면 충돌 및 사고의 위험 발생

프로그램 연동, 호출의 신뢰성 문제

다른 사람의 오픈 소스 또는 연동 API 프로그램의 취약성을 의심하고

직접 인공지능 프로그램을 개발하는 개발자가 있을까?

연동해도 제대로 동작하는 지도 문제

결국 검증과 충분한 테스트를 거쳐야 함

그렇다고 해서 안전성을 보장하는 것은 아님

오류, 장애, 실수, 결함 → 사이버보안영역

사이버 공격은 시스템의 오류, 장애, 실수, 결함 등의 취약점을 이용하여 침입
단순 응급처치가 아닌 근본적인 문제 해결 방식으로 접근 필요

3 상생의 기술

인공지능 기술이 발전한 이유

연산 장치의 고속화, 병렬 처리 → GPU

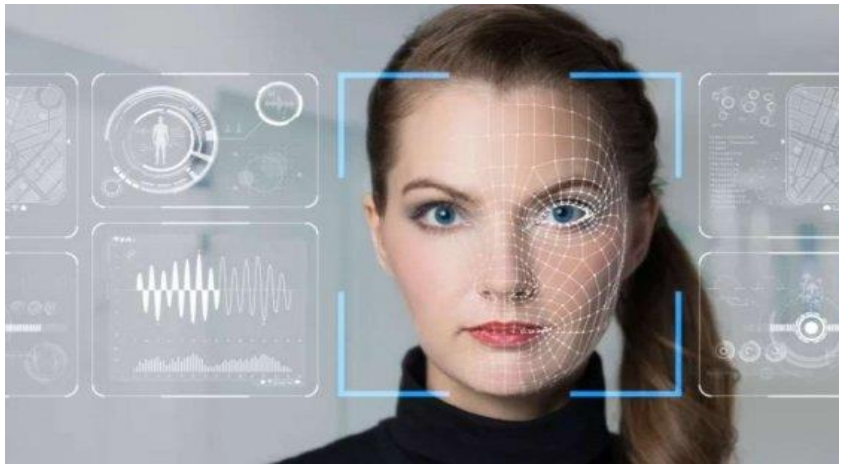
메모리의 무한 증가 → SSD, DRAM

초고속 인터넷 연결 → 5G

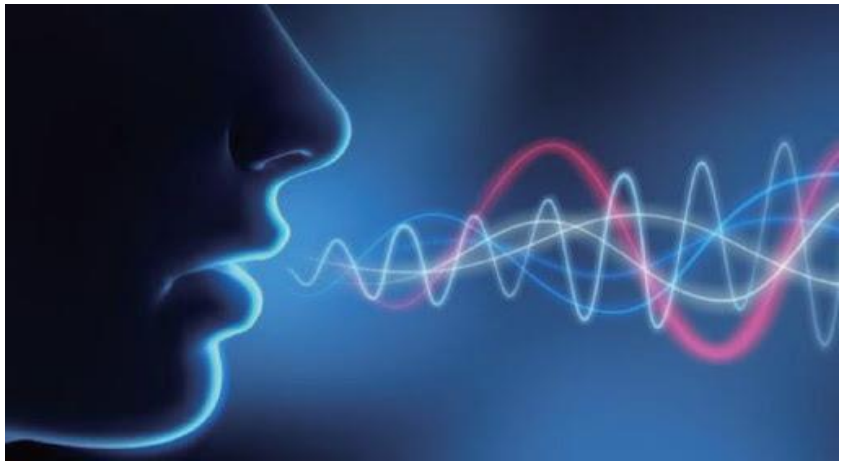
새로운 알고리즘의 탄생 → Deep Learning

글로벌 기업의 적극적인 투자, 각국 정부의 관심 증대 등 상호 이익이 합치됨

인공지능 활용 분야



패턴 인식



음성 인식

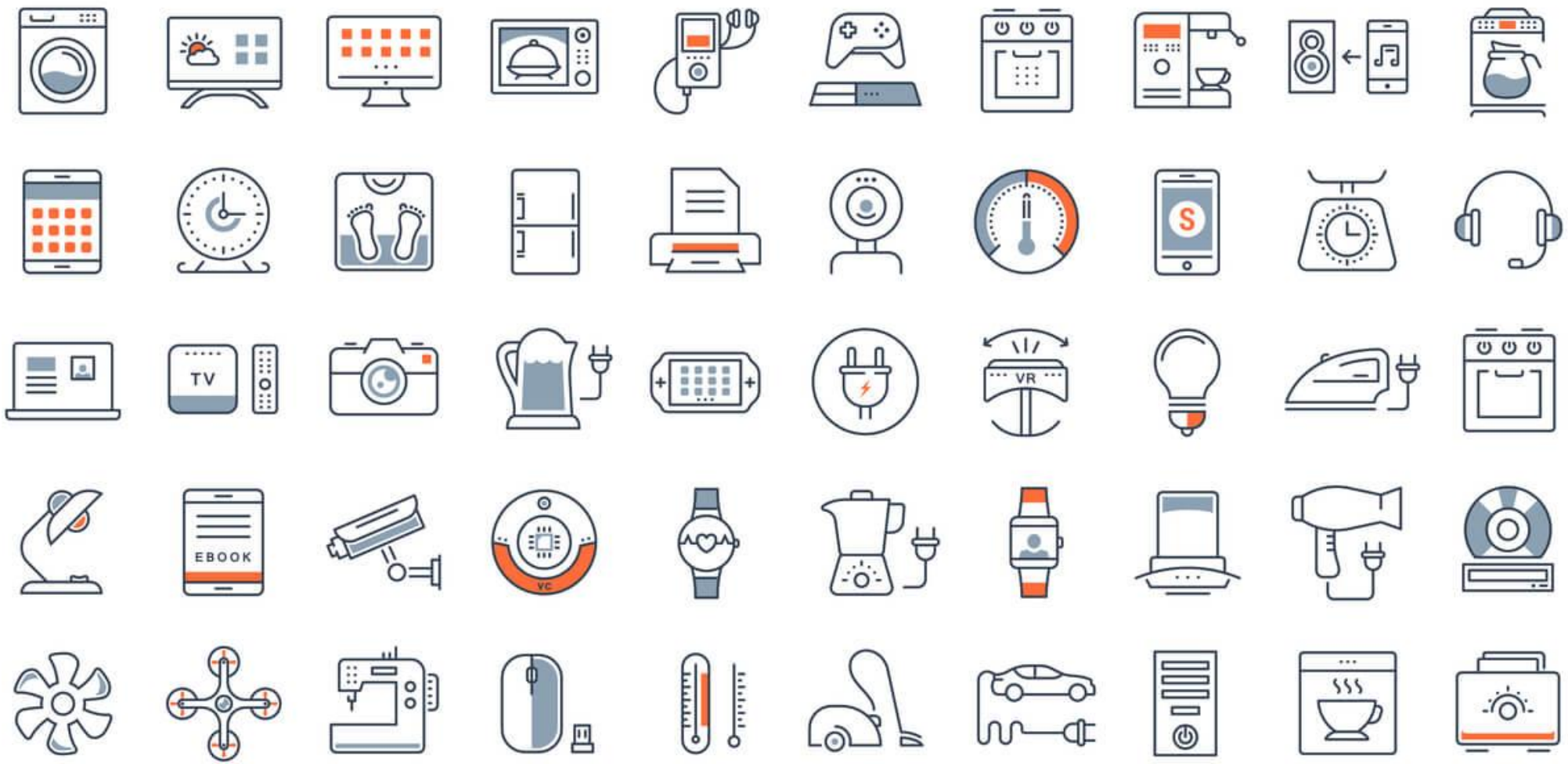
비서, 생활정보 알리미

고객 관리

이외에도, 활용분야는 많다

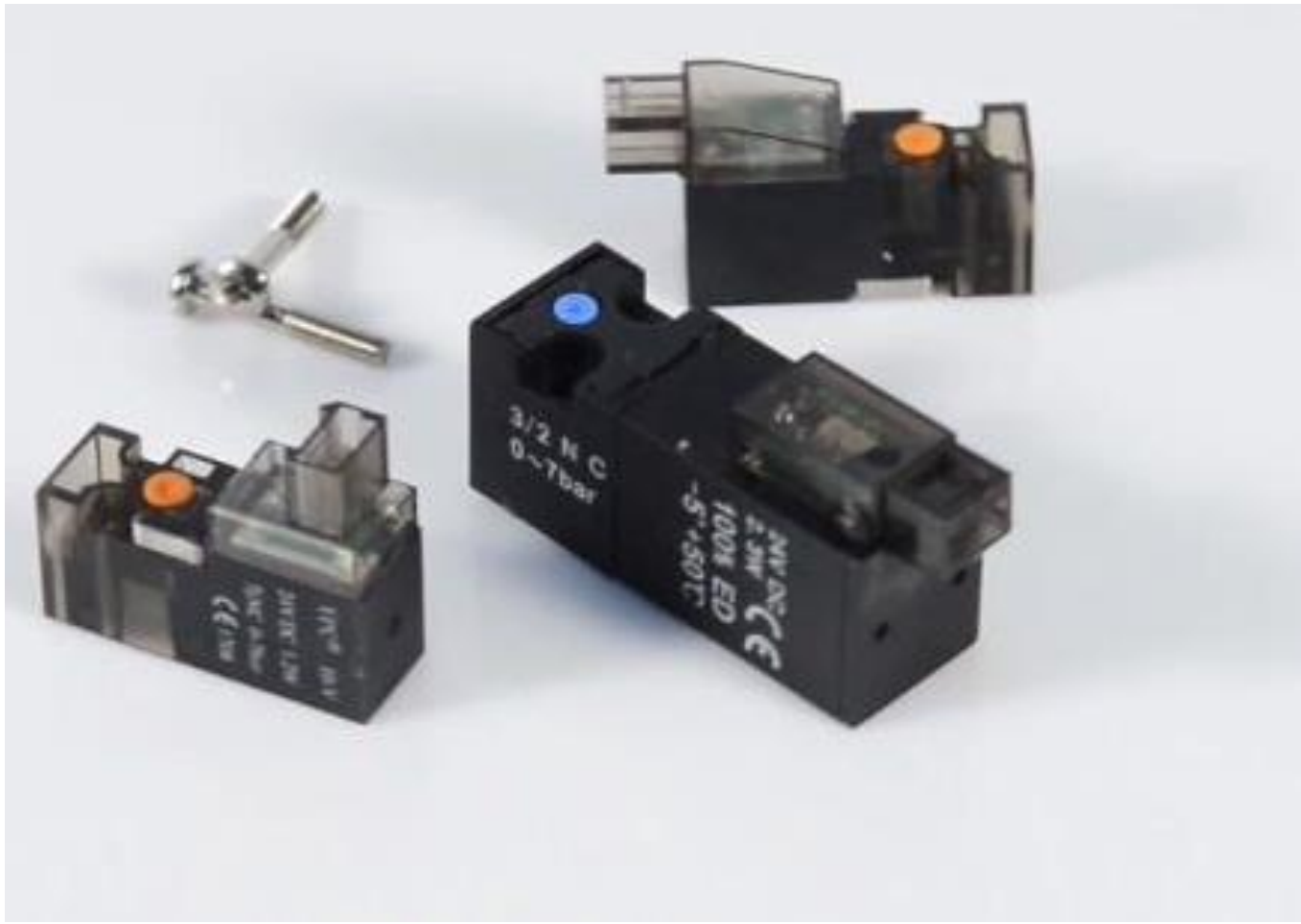
웨어러블 디바이스

이외에도, 활용분야는 많다



사물인터넷(IoT) 기기

이외에도, 활용분야는 많다



센서, 밸브, 감지기 등

소론 : 안전한 AI 시스템 설계 필요

패턴 인식

네트워크

데이터 셋

어플리케이션

가상 현실(Virtual Reality)

Cyber Range구축 Search

모의 침투 시험(Penentration) Search

보안 관제 Search

증강 현실(Augmented Reality)

관제 Visualization Search

정보보호 제품 형상관리 Search

사이버보안 교육 & 훈련 Search

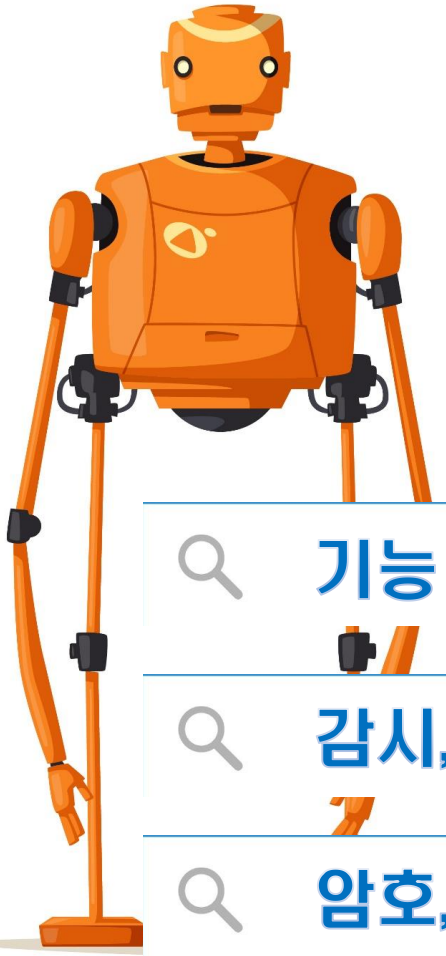
핀테크(Fintech)

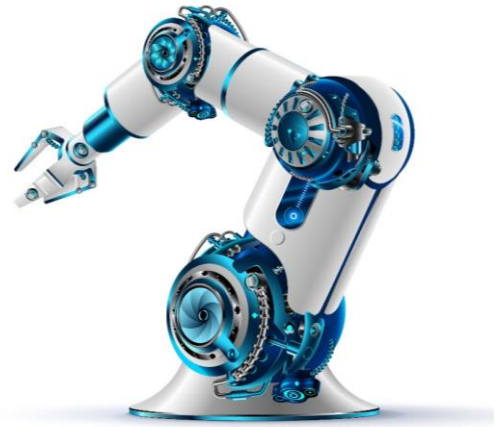
ID, Password & 공인인증서 Search

매체 인증, 생체 인증 Search

블록 체인, 비트 코인 Search

로봇(Robot)





기능 중단, 마비 방지	Search
감시, 정보 유출 방지	Search
암호, 침입 탐지, 보안 인증	Search

스마트 카(Smart Car)

자율/무인 주행 Search

커넥티스 서비스 보안 Search

해킹 보안, 취약점 분석 Search

드론(Drone)

Hijacking, 무선통신 보안 Search

위치 정보, 지리 정보 등 Search

드론용 레이더 Search

군사용 드론(Dhrone)

정찰/첩보 데이터 Search

재밍, 스푸핑 등 전자파 보안 Search

GPS 보안 Search

스마트 펙토리(Smart Factory)

장애, 결함, 고장 검증 Search

신뢰성 테스트 Search

위험 평가, 위험 관리 Search

스마트 시티(Smart City)

지능형 교통정보(ITS) 보안 Search

5G, 6G 등 보안 무선통신 기술 Search

보안 관리(CCTV, 감시, 추적) Search

스마트 에너지(Smart Energy)

SCADA 보안 Search

송배전시스템 보안 Search

기반시설 보호(취약점 분석 등) Search

헬스케어(Health Care)

개인정보 & 의료 정보 보호 Search

원격 진료 보안 Search

랜섬웨어(워너크라이 등) 대책 Search

생명공학(Bio)

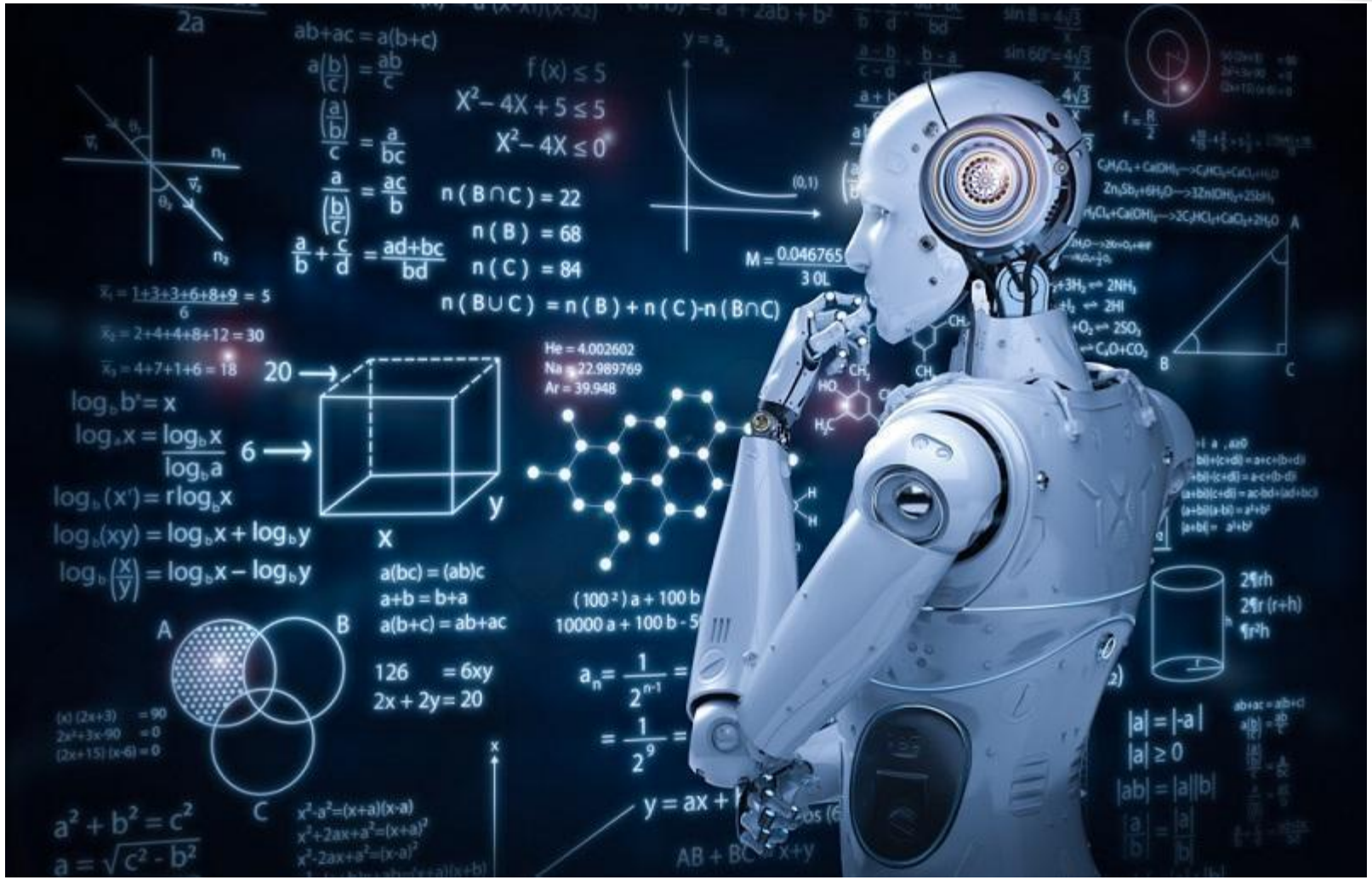
저작권, 특허 Search

산업 기밀 유출 보안 Search

생명 윤리 Search

4 결 언

인공지능 학습과 훈련 : 경험과 노하우



아직은 유아기이므로 많은 것을 올바르게 학습하고 경험할 수 있도록 해야 함

인공지능 학습과 훈련 : 샌드박스, 허니팟 운영

시장에 나오기 전에 충분한 실험을 할 수 있는 공간 마련

인공지능과 보안 → 산업 발전에 기여

일자리창출과 청년 실업 해결에 앞장서야 함

인공지능과 보안 → 국가 안보에 기여

사이버공간에서 안심하고 활동할 수 있는 기반 마련

인공지능과 보안 → 국민에게 신뢰를 받는 기술

인공지능을 사용하면서 걱정과 불안을 종식시켜야 함

인공지능과 보안 → 협업, 연동이 가장 중요

인공지능 또는 사이버보안 홀로 연구가 불가능 : 협업

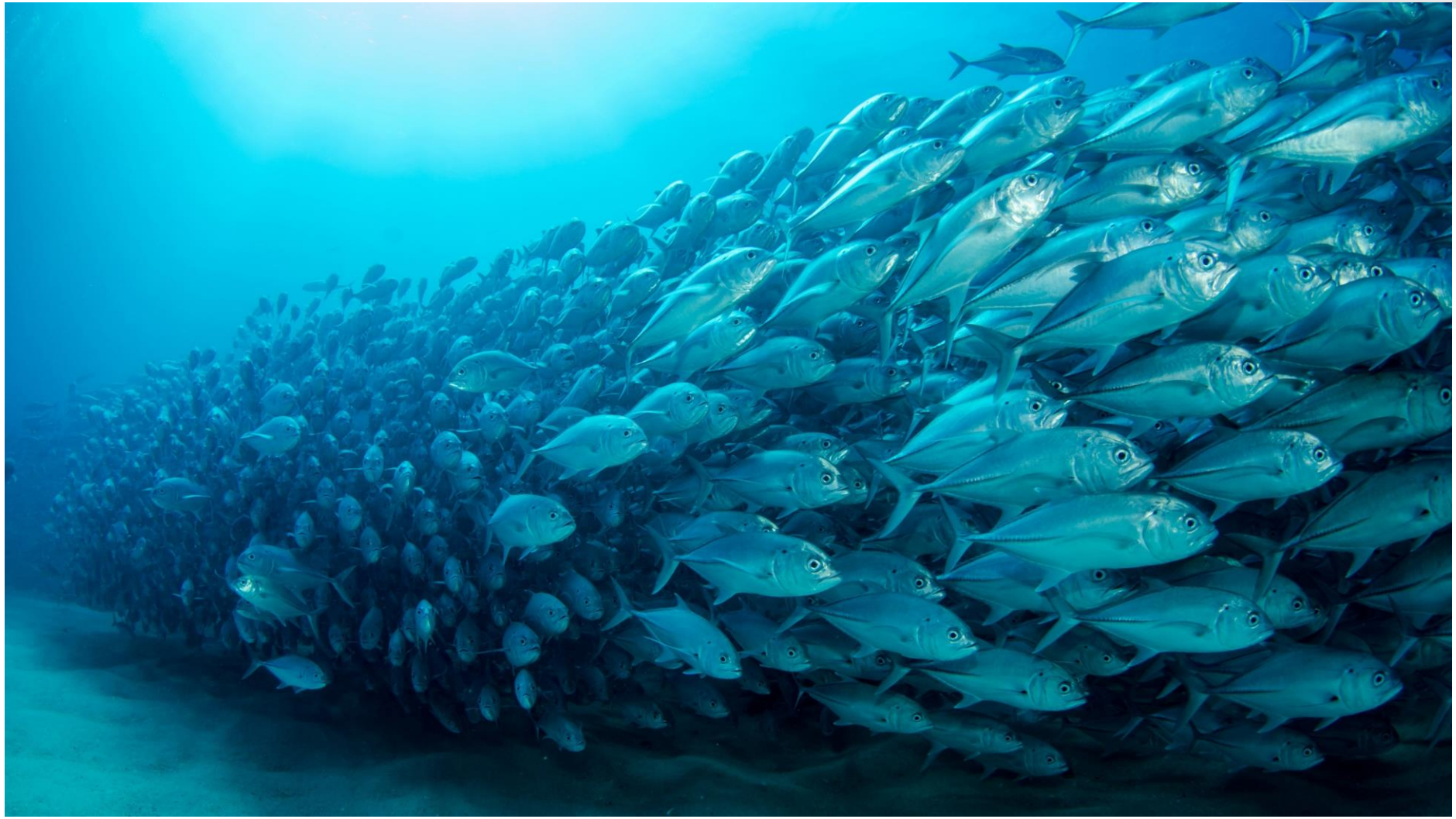
보안은 아킬레스 건이 아닌 함께 풀어야할 숙제

이제는 인공지능 설계시 사이버보안을 먼저 설계에 반영

결언 : 동전의 양면

서로가 다른 것 같지만 하나가 되어야 활용 가능

결언 : 수어지교



물고기와 물은 반드시 함께 가야 함

감사합니다.