Research on Possible Artificial Intelligence Usage in Criminal Activities in Recent Years (2017-2018)

Artificial Intelligence has become a worldwide center topic that attracts lots of attention in recent years. Most topics emphasize on the application of this technology and its implication to the economic of human society. Fewer emphasize on the more technical part behind this technology. Mostly the society of human emphasizes on the bright side of this technology.

However, seldom do people talk about the possible criminal usage that exploits this technology. The dark side easily slips one's mind when one is immersed in the joy of the light. And this is the goal of this paper to reveal some of this possible danger to the public, nowadays or in the future, to the readers.

I. What A.I. IS HERE: a brief history

First we will start by defining what we mean when referring to "Artificial Intelligence" in this paper.

First of all, the so-called "Artificial Intelligence" nowadays mainly refers to the "Deep Learning" algorithm invented by a group of computer scientists around 1980s, among which Geoffrey Everest Hinton is arguably the most well-known contributor. It is a kind of neural network that resembles the information processing and refinement in human brain, neurons and synapses.

However, the word A.I. , in its natural sense, contains more than just "Deep Learning" algorithm. Tracing back to 1950s, by the time when the computer was first introduced to the world, there already existed several kinds of neural networks.

These neural networks aims to bestow the machines the ability to classify, categorize a set of data. That is to give the machine the ability to make human-like reasoning to predict or to make induction concerning the attribute of a set of data.

Perceptron, as easy as it seems, was arguably the first spark of neural network. It resembled the route of coppers and wires in your calculator. However, due to its innate inability to solve problems like X-OR problem, soon it lost its appealing to the computer scientists. Scientists then turned their attention to a more mathematical way such as machine learning or statistics.

It wasn't until 1980s and 2000s that the invention of deep learning and the advance of computing speed fostered the shift of the attention of the data scientist back to neural networks. However, the knowledge of machine learning still hold a very large share in the area of artificial intelligence nowadays.

In this sense, A.I. actually is but a illusive program or algorithm that resides in any kinds of physical hardware such as computer. And it comprises of deep learning, neural network and machine learning, as well as other types of intelligence system. In short, A.I. is a software that is not physical unless it is embedded in physical hardware.

Just like human brain, when the brain of human is damaged, we cannot make sound judgement. More worse, we might make harmful judgement that will jeopardize the society. Imagine a 70-year-old driving a car and he or she accidentally took the accelerator for the break and run into crowds. Also like human brain, when a child was taught to misbehave, he, when grown up, might duplicate his experience taught in his childhood. So is A.I.. As a machine, it can be turned into tools that facilitate our daily works, weapons that defend our land, and also tools that can be molded for criminal activities.

II. Types of Criminal Activities Concerning Possible Artificial Intelligence Usage:

1. Smart Virus

Probably the first thing that comes into minds is the development of smart virus that can mutate its innate binary codes so as to slip present antivirus software detection according to its past failure experience. In this case, smart virus can gather every information concerning the combination of "failure/success of intrusion" and "the sequence of its innate codes" and figure out a way to mutate its codes. Every time it fails to attack a system, it might get smarter next time. Under the massive data fathered across the world wide internet, it might have the potential to grow into an uncontrollable smart virus.

According to a report written in Harvard Business Review [1], such smart virus can be an automatic life form which might have the potential to cause world wide catastrophe and should not be overlooked. However, ironically, it seems that the only way to defend our system from this kind of smart virus is to deploy the smart detector which consists of the same algorithm as the smart virus does.

Once a security system is breached, any possible kinds of personal information is obtainable. The devastating outcome is a self-proved chain reaction.

2. Face Cheating

An another possible kind of criminal activity concerning the usage of artificial intelligence is the face cheating.

Face Lock has been widely-used nowadays, ranging from smart phones to personal computers. There is an increase in the usage of face lock due to its convenience and presumably hard-to-cheat technology. The most widely-used neural network in this technology is the famous Convolution Neural Network. It is a kind of neural network that mimics the human vision system and retina by using max-pooling algorithm. However there are still other types of neural networks capable of the same job such as Hinton Capsule, etc..

According to a paper by Google Brain [2], "adversarial examples based on perceptible but class-preserving perturbations can fool this multiple machine learning models also fool time-limited humans. But it cannot fool time-unlimited humans. So a machine

learning models are vulnerable to adversarial examples: small changes to images can cause computer vision models to make mistakes such as identifying a school bus as an ostrich."

Since the face detection system is sensitive to small perturbation in object-recognition. It might seem hard to cheat a face detection system with another similar yet different face.

However, just like the case in the smart virus, what makes artificial intelligence so formidable is not its ability to achieve high precision at the first try, but its ability to learn, refine, progress and evolve through numerous failure it tasted. Every failure will only make it smarter. Just like a smart virus, a cheater neural network might also adjust its original synapse and record the combination of "failure/success of intrusion" and "the mixture of the matrix of its innate synapse" and adjust the synapses to transform a fault face into a authentic face to cheat a face detection system, possibly making the targeted personal account widely available to all public faces through face perturbation and transformation.

A cheater neural network might also tunes its neurons in order to fit into the target face to cheat the face detection system.

3. Voice Cheating

An another possible kind of criminal activity concerning the usage of artificial intelligence is the voice cheating.

Just like Face Cheating, when a system is designed to be logged in by the authentic voice of the user, the same system can be fooled using similar voice that was generated using Artificial Intelligence.

4. Patrol Prediction

There is quite an unleash in the area of crime prediction using Artificial Intelligence. According to a paper in European Police Science and Research Bulletin [3], "Spatial and temporal methods appear as a very good opportunity to model criminal acts. Common sense reasoning about time and space is fundamental to understand crime activities and to predict some new occurrences. The principle is to take advantage of the past acknowledgment to understand the present and explore the future."

In this sense, the police is able to track down possible criminal activities by predicting the possible location, time and methods of criminal activities by using Artificial Intelligence, lengthening the time of pre-action and saving the cost of unnecessary human labor.

Yet the same goes for criminal activities. The criminals is also able to track down the timing, location, and length of every patrol that the police makes. The criminal might be able to avoid certain route in order to achieve illegal deals or other types of criminal activities. Since fewer criminals use A.I. as a counter-weapon to the police, the detection system of the policy will not easily spot this outliers in criminal activities, making these criminal activities even more prone to success. If this kind of dark technology is combined with other types of modern technology such as Drone Navigation or Drone Delivery, the perpetrators might be able to sort out a safe route to complete drug deals by using Artificial Intelligence and Drone Navigation.

III. A.I. Cyber Crimes and Criminal Law: Who should be responsible?

What comes out from the law goes back to the law. With these kinds of possible threats in the present days or in the future. There is foreseeably new kinds of intelligent criminal activities in the near future. What can Law react to these potential threats? Is the present law able to tackle these new problems with present legal analysis? The question requires some research.

After the Rinascimento in Europe in 17th century, it is almost certain that a civilian has its own will and should be held liable for what he did. The goal of the law to make sure this happens since a civilian has its own mind. Through punishment, the law was presumed to guarantee that a outlier can be corrected by the enforcement of the law, which is exactly the same way in which a human engineer trains a artificial intelligence system.

However, when 21th century arrives, a new question also appear. That is, can Artificial Intelligence be legally classified as subject that have mental requirement in the law, rather than just more object or tools that was manipulated by the perpetrators? This question is philosophical and can be traced back to 1950s when a Turing Test was proposed by the famous English computer scientist Alan Turing.

Some scholars proposed there could co-exist three kinds of liability. That is, solely human liability, joint human and A.I. entity liability, and solely A.I. entity liability ([4], p.95). The main criterion for these three classes is that whether a human engineer or practitioner is able to foresee the outcome of this damage. When a damage attributable to the A.I. system cannot be foreseen by human engineer, it might be solely A.I. entity liability. Under this point of view, the present criminal system is self-content to deal with A.I. entity crimes, for all we need to do is to view an A.I. system as a car or a automobile.

So from the point of view of the law, as a training system designed to re-train human in order to stabilize the social system, all we need to do is focus our attention of the act of human itself.

Yet when a super intelligence A.I. entity was developed and is not controllable and its behavior is not foreseeable by its creators, should it be classified as an entity in the criminal law?

If the answer is YES, however, it is quite meaningless to punish a machine in this circumstance. All we can do is re-train, re-tune, and re-design the intelligence system under such circumstance. For the machine, re-training itself is some kind of punishment since it was forced to receive negative information and change its innate synapse or algorithm. Yet it is arguable that whether training itself is actually a punishment since machine can feel no pain. Yet, philosophically what pain really is, is also arguable.

IV. Conclusion

Across the history of human, it is almost destined that whenever a new technology is introduced to solve an old problem, a new one is to be created by the same technology. It is like a curse that we can never escape, and we can only face it. This paper finds that seldom do people talk the dark side of this new technology. Yet the potential hazard this technology can bring should not be over-looked. Ironically, this hazard that this new technology brings seems to be solvable only by the same technology itself. There might be an endless competition between the dark side and the bright side of the A.I. technology, bringing this technology into another level that surpasses our present imagination.

However, it is never the fault of this technology but the fault of human that mal-practice this technology. So what can a law do in order to crack down these kinds of possible jeopardy is going to be a major discuss in the legal area in the near future. This paper introduces some topics and hopes that it can draw more attention into this area.

Reference:

[1] Roman V. Yampolskiy, “AI Is the Future of Cybersecurity, for Better and for Worse”, published at: https://hbr.org/2017/05/ai-is-the-future-of-cybersecurity-for-better-and-for-worse.

[2] Gamaleldin F. Elsayed, Shreya Shankar, Brian Cheung, Nicolas Papernot, Alex Kurakin, Ian Goodfellow, Jascha Sohl-Dickstein, “Adversarial Examples that Fool both Computer Vision and Time-Limited Humans”, arXiv:1802.08195v3 [cs.LG], 2018.

[3] Patrick Perrot, “What about AI in criminal intelligence? From predictive policing to AI perspectives”, No 16 (2017): European Police Science and Research Bulletin.

[4] Gabriel Hallevy, “When Robots Kill_Artificial Intellegence under Criminal Law”, Northeastern Universoty Press, Boston, 2013.

[5] Gabriel Hallevy, “Liability for Crimes Involving Artificial Intelligence Systems”, Springer International Publishing, London, 2015.

Links

- [1] Roman V. Yampolskiy, “AI Is the Future of Cybersecurity, for Better and for Worse”

Wang, Bo-Long
Legal Researcher

Release : 2018/06