The Potential of AI to Propose Security Countermeasures

HOSOMI Itaru

Abstract

As technology evolves, enhancing our lives in a myriad of ways, so too does its dark side. Today, cyberattacks are becoming ever more sophisticated and organized, and while the knowledge and experience of human analysts remains critical in preventing these attacks and developing effective, concrete counter-measures, cyberattack detection technology based on machine-learning AI is becoming increasingly effective. Recently, a number of startups in North America have developed machine-learning AI — such as those based on deep learning. In this paper, we will discuss the potential of logical inference AI as a tool for coping with the kind of complex, unformatted attacks that are expected to become prevalent in the future.

Keywords
artificial intelligence, logical inference, security operation, cyber kill chain, SIEM, security orchestration and automation

1. Introduction

The threat posed by cyberattacks is becoming more serious every year. Since the first confirmed attack in 2002, targeted attacks have inflicted significant damage in a number of countries around the world. In 2013, a new threat arose with the proliferation of ransomware. Attack methods have become more varied and are now specifically individualized according to targets, while the sophistication of incubation and evidence removal continues to evolve. To combat these attacks, artificial intelligence (AI) technology is now being utilized for automatic detection of the existence and behavior of malware and is becoming better able to perform this task as it evolves. AI technology that uses machine learning is able to detect malware - even subspecies and unknown ones - more effectively than conventional methods based on signatures and rules and is now expected to play an important role in protecting against unpredictable and ever more varied attacks. However, it is still difficult to solve everything with machine learning, and it is expected that it will be quite some time before human analysts are taken out of the equation. But why is that so? In this paper, we will focus on a number of questions we should consider when we utilize AI for cybersecurity and discuss the potential of logical inference AI to solve the issues raised by asking those questions.

2. Why Is AI Technology Essential for Cybersecurity?

2.1 Increasing Threat of Cyberattacks Due to Industrialization and AI Technology

As shown in the schematic diagram in **Fig. 1**, cyberattacks are becoming increasingly varied. While there are still many indiscriminate attacks such as malware distribution and fraudulent emails, sophisticated targeted attacks that specify the targets to be attacked are now becoming a serious menace. Cyberattacks in recent years have been distinguished by their highly organized and industrial-scale properties. Reportedly, personal information and a variety of malware used for targeted attacks are widely, readily, and inexpensively available in the black market to facilitate the reconnaissance and weaponization that are the first stages of the cyber kill chain (**Fig. 2**).

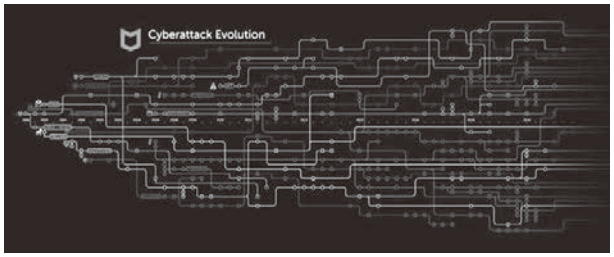

Fig. 1 Evolution of cyberattacks according to McAfee.[1)]

*1 Online entity that takes advantage of security vulnerabilities
*2 Command and control, remote control from outside

Fig. 2 Cyber kill chain.

Now, hackers are enjoying a situation where they can launch targeted attacks against numerous targets in short periods of time by using tools available on the black market. This has made the boundary between indiscriminate attacks and targeted attacks ambiguous. It is now understood that conventional human resources and response speeds will be unable to keep pace with the rapid changes in cyberattacks. It is this realization that is leading security specialists to place their hopes in AI technology where rapid progress is being made.

There is also another factor to consider. It is unavoidable that the hackers will also use AI technology. To counteract this, AI technology specifically tailored for protection will be necessary. In the Cyber Grand Challenge held by the Defense Advanced Research Projects Agency (DARPA) in 2016, participating teams fought fully automated battles with one side taking the offence and the other defense. Everything from detection of vulnerability and commencement of attacks to patch application to prevent attacks much faster than would have been possible conventionally. To cope with attacks at speeds so high they exceed human capability, similarly high-speed countermeasures are required.

2.2 Utilization of AI Technology for Protection

Then, how should we utilize this promising AI technology? As a matter of fact, it has already widely used for detection of malware, and its effectiveness has already been established. One proof of its effectiveness is that in July 2017 Google announced that they would integrate Cylance's AI technology into VirusTotal, which is a malware detection service run by Google. IBM is also trying

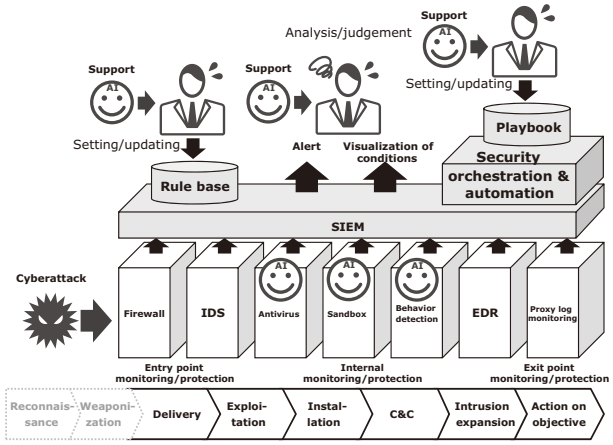

Fig. 3 Utilization of AI in security procedures.

* An artifact that indicates computer intrusion

Fig. 4 Example of the basic steps of a playbook.

to demonstrate the effectiveness of its AI technology for intelligent search engines that comprehensively manage huge amounts of threat data using Watson for Cyber Security.

Clyance's CylancePROTECT and NEC's automated security intelligence (ASI) self-learning system anomaly detection technology fall into the category of sensors that detect malware. The introduction of security information and event management (SIEM) is now underway as a means of comprehensively assessing attacks based on multiple sensors. The current SIEM systems function almost solely on a rule basis. The key to effective operation of SIEM is timely updating of rules. AI is ideal for and is expected to improve the effectiveness of SIEM operation and support comprehensive threat assessment (**Fig. 3**).

In terms of improving efficiency and quick response, startups that offer a type of solution called security orchestration and automation (SOA) have been attracting attention in the United States since about 2014. The representative startups include the US's Phantom Cyber, also the US's Demisto, and Israel's Hexadite. In SOA, counter procedures on the defense side called playbooks are defined in advance. According to these procedures, SOA can automatically perform information gathering, analysis, and execution of countermeasures (**Fig. 4**). Here too, it is expected that AI will play a crucial role in adaptive planning and updating of playbooks.

3. Why Is Only Machine-Learning AI Insufficient?

3.1 Because You Need a Huge Amount of Learning Data

Instead of being fed with knowledge manually, machine-learning AI needs a massive amount of learning data. Deep learning, in particular, requires more learning data than other machine-learning systems. In other words, before a machine-learning AI can detect a new type of malware and other threats that are significantly different from conventional ones, it must accumulate an enormous amount of data in order to detect the signs of malware or other threats. With targeted attacks directed at specified targets, collecting enough data may simply be impossible.

3.2 Because You Need to Know the Reasons for the Results

Another characteristic of machine-learning AI including deep-learning AI is that it is capable of assessing data that is different from any learning data. In other words, even when a subspecies of malware emerges, the AI can detect it by uncovering what it has in common with previous malware. However, if the detected malware does not correspond with the properties of any of known malware, the AI will not tell us why it made its assessment.

3.3 Detection Is Not the Only Important Issue

Current machine learning is suitable for detection of malware and abnormal changes of conditions because it basically excels in distinction and classification of entities. Nevertheless, when an assessment based on past context or a countermeasure proposal derived from multiple protocols is required, it is difficult to achieve this using conventional machine learning. For example, AlphaGo, which overwhelmed human players in the game of Go, used deep learning to learn the moves human players took in each position. When it thought about its own moves, however, it used a different technology called Monte Carlo methods.

4. Why Are Human Analysts Necessary Even in the Future?

4.1 Because There Are Things Only Humans Can Do

As already mentioned, machine-learning AI is not good at systematic intelligent processing such as planning countermeasure procedures. Neither will it be able to make assessments based on socially accepted common sense and human psychology; these will remain in the domain of human experts for quite some time. Moreover, ultimately only humans can take responsibility for the final decision in terms of its legal and cultural ramifications. In addition, when it is necessary to obtain data from objects subject to permanent monitoring, negotiations between humans will be required in order to get the necessary permission. Consequently, human intervention will still be necessary even when attacks become even more diversified and higher-speed.

In currently employed entry/exit measures, analysts must determine the truth or falsehood of alerts. When an intrusion is detected, a sizable number of analysts spend at least a few days and probably more than a month investigating and dealing with it, which can easily cost as much as a million dollars[2)]. It is important that attacks be detected and isolated after an intrusion and normality be restored as soon as possible. SOA, which is expected to help accomplish this goal, allows you to automate information gathering and countermeasure planning according to a playbook, but the playbook itself needs to be created by humans in accordance with the actual conditions of the attacks. At the same time, security giants such as IBM and HPE insist that countermeasures based solely upon established playbooks are difficult to implement in an environment where the methods and modes of attack are becoming more diversified and individualized, meaning that evaluation by human analysts will continue to be required in the future as well.

4.2 Why Does AI Have to Answer the Whys?

If conventional machine learning is incapable of explaining the reasons for the results in an easy-to-understand manner, then why do we have to understand the reasons in the first place? It is precisely because it is we humans who will decide what measures will be taken and take responsibility for that determination. Furthermore, it is necessary to be able to explain to stakeholders and customers the nature of an attack, how it occurred, and what countermeasures have been taken.

5. Potential of Logical Inference AI

NEC is working to develop AI able to collaborate with humans to solve problems by contextualizing the situations within a wider perspective - as in responses to security incidents. To achieve this goal, methods of expression are required that can be understood by both AI and humans. The AI also needs to be capable of running an analysis that incorporates human opinions about the issues.

When applying the AI developed by NEC on an inci-

dent response basis, it will be necessary to build a structure in which the AI is responsible for drafting playbooks as and when required, like those used for SOA according to attack conditions, as well as conducting automatic investigation and confirmation, while anything that should be handled by humans will be sent to the analysts. To draft a playbook, the first thing that is required is materialization of a cyber kill chain that shows how the attack in question is going to be carried out.

To meet these requirements, NEC is studying the feasibility of logical inference AI, which has a different origin than machine-learning AI. While machine-learning AI uses knowledge unintelligible to humans who simulate the data characteristics on mathematical models, the logical inference AI uses knowledge expressed with symbols and logical expressions that are intelligible to humans. The once popular expert systems that used strictly defined knowledge eventually were abandoned due to their lack of flexibility and the difficulty of managing them. More recently, however, technologies that feature both logical accountability and reasoning capability have been developed.

In addition to its ability to show how its results have been derived in a manner comprehensible to humans, the logical inference AI can add to and revise its knowledge in order to improve its ability to draw inferences. Thanks to this technology, the AI can infer what kind of operation is being executed by the malware or by attackers by drawing on its store of knowledge about cyberattacks to collect as much data as possible regarding relevant incidents as soon as an anomaly is detected by the sensor. The AI derives the flow until the objective of the attack is finally accomplished. To verify that flow, the AI uses the incident data it has collected to confirm the inferred operations at each step and the process conditions. When the AI determines that the derived flow is by and large correct, it stops that flow and now derives the procedures until the countermeasures are complete. Finally, the results are verified in cooperation with human analysts.

To create this technology, a great deal of R&D is still required. To get a basic idea of this, let's take a look at an example in which a capture the flag (CTF) problem in a security competition was solved with logical inference. Showing that example giving a question to find flags (lines of specific characters), **Fig. 5** explains how every possible procedure until the flags were discovered was derived using logical inference (note that the actual internal expressions were expressed with functional expressions of computer programs). You can tell from this example that the derivation is comprised of sequential operations and conditions as is the case in the cyber kill chain in Fig. 2 and the playbook in Fig. 4. There may be cases the text files can be found or the flags can be directly found in the packet data. These possibilities are automatically verified using various tools and commands. If a mistake is made, the procedure is revised and the operation continues until the flag is finally found. As for technical issues, some work is still required - such as building sufficient knowledge that covers all possible eventualities in a wide variety of conditions, establishing a procedure selection method ideal for reaching a correct solution with as few verifications and revisions as possible.

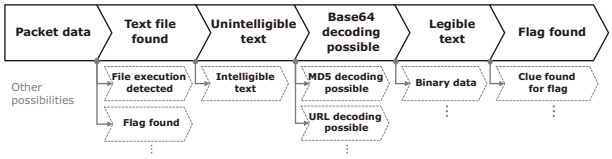

Fig. 5 Generation image of solving CTF problem.

Now, we are planning to expand the problem-solving approach by inserting candidates for procedures and conducting verification using logical inference, as shown in this example, into the plotting of the overall picture (cyber kill chain) of an attack and the drafting of the counter procedure (playbook). In CTF, however, there are clear answers and all the necessary data that can be used as evidence, while in actual cyberattacks only the hackers know the correct answers and it can hardly be expected that all the necessary evidence can be gathered. These points must be taken into consideration. Although our logical inference AI will acquire and update the knowledge for inference by using machine learning from threat information and data in the same manner as IBM Watson, we think that it is important to improve the ability of the technology to acquire knowledge from human analysts as well.

6. Achieving AI That Can Tell You Why

Through the R&D into logical inference AI and its application to cybersecurity, NEC is aiming to achieve AI that can show inferred attack methods to demonstrate why it is necessary to respond to incidents at a given moment, show inferred measures to show why that response is appropriate, and explain the validity of the response and the countermeasures based on its own research and analysis, as well as the evaluation of human analysts. In so doing, we will reduce the time and labor required for analysts to make a comprehensive evaluation - something that is not supported by conventional machine-learning AI - and contribute to the achievement

of solutions that can manage the increasingly diversified and sophisticated cyberattacks expected in the future.

* IBM and IBM Watson are trademarks of International Business Machines Corporation in the U.S.
* All other company names and product names that appear in this paper are trademarks or registered trademarks of their respective companies.

Reference

1) Brian Dye: Changing Cybersecurity for a New Era,2017.4.7
https://www.slideshare.net/scoopnewsgroup/brian-dye-changing-cybersecurity-for-a-new-era
2) Ponemon Institute: 2016 Cost of Cyber Crime Study & the Risk of Business Innovation,2016.10
https://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf

Authors' Profiles

HOSOMI Itaru
Principal Researcher
Security Research Laboratories

Information about the NEC Technical Journal

Thank you for reading the paper.
If you are interested in the NEC Technical Journal, you can also read other papers on our website.

Link to NEC Technical Journal website

Japanese

English

Vol.12 No.2 Cybersecurity

- Building Futureproof Security to Support Business Safety and Reliability -

Vol.12 No.2
January 2018

Special Issue TOP