ISSN: 2664-9640

Cyberspace security attack-with-defense drill and CTF competition based on AI

Yichen Chen, Junteng Liu, Zhiyou Yu

School of Information, Southwest Petroleum University, Chengdu, 610500, China

Abstract

In today's society, the exploration and development of Artificial Intelligence (AI) has reached an unprecedented height. When AI has a far-reaching impact on big data, blockchain, and other fields, it is also making major changes in the field of Cyberspace Security. Based on it, this paper will discuss the cyberspace security attack-with-defense drills and CTF competitions in the context of AI. First, it introduces the era background and technical background of cyberspace security attack-with-defense drills; Then it points out the application of some emerging AI technologies in cyberspace security, and explains how AI technologies can break through the traditional attack-with-defense drills during network protection projects; Finally, a new model of CTF (Capture The Flag) cyberspace security competition under AI technology is given. The use of these three aspects reflects the "double-edged sword" benefits of AI technology in cyberspace security and achieves the purpose of promoting application through learning and promoting war through an application. In the non-stop game, cyberspace security and AI make common progress together, improving the level of technological innovation, so that they can complement each other, and finally promote the development and progress of cyberspace security.

Keywords

Artificial intelligence, cyberspace security, attack-with-defense drill, CTF.

1. Introduction

With the rapid development of the Internet, from the government to enterprises to individuals, hundreds of millions of assets are deployed on the network, which greatly facilitates our lives. However, these assets will also become the preferred target of attackers. In recent years, many cyberspace security incidents have occurred at home and abroad, Such as Apache Log4j2 remote code execution vulnerability, "turtle" DNS hijacking incident, JustDial database information leakage incident, ios operating system "backdoor" incident, etc. There are even attacks supported by national background, which show an obvious upward trend, directly reflecting the increasingly severe Cyberspace Security Environment in the Internet era. The continuous development of AI technology has not only greatly promoted the cross-integration of computer science and other disciplines such as finance and medical care, but as the most innovative key technology in the future, AI has also gradually changed the attack-with-defense drills that subverted the traditional cyberspace security field and competition mode.

DNS (domain name system, as one of the most important test objectives in cyberspace security attack-with-defense drill, its traditional cyberspace security problem often lies in DNS hijacking or DNS pollution: The domain name server provided by IPS records the domain name, IP address, etc. Once these records are tampered with, the traffic of the defender will be redirected to the address specified by the attacker, resulting in DNS hijacking; DNS pollution also means that the attacker uses the difference in the transmission time of the data packets to forge a wrong "DNS response" and return it to the client. Under the AI technology, a new type of DNS

ISSN: 2664-9640

secret stealing attack is derived, and its specific attack methods are as follows: The attacker simulates APT (Advanced Persistent Threat attack, also known as directed threat attack) organization, With the good concealment and penetrability of the DNS protocol, using AI's ability to identify specific data, implement data theft and complete the attack[1].

Traffic analysis is a classic problem in cyberspace security attack-with-defense drills and CTF competitions. Traditional traffic analysis is based on the situational awareness platform products of major security vendors (Ruijie Networks Big Data Security Platform RG-BDS, Wangyu Network security situational awareness platform, Mingjian network security situational awareness notification and early warning platform, etc.) to conduct malicious attack traffic early warning, quick response; Afterwards, traditional traffic analysis can be performed using tools such as Wireshark to traceability for evidence collection. In the context of AI technology, autonomous traffic analysis has become an emerging technology, namely "traffic +", endowed with the ability of intelligent learning of traffic, combined with technologies such as honeypots (a trapping network to deceive attackers), the network defenders can change from "passive defense" to "active defense", and conduct attack defenses more effectively.

It can be seen that AI technology is a "double-edged sword" in the field of cyberspace security. While generating more security problems, it also gives unlimited possibilities to the security field. This paper will discuss and analyze the cyberspace security attack-with-defense drills and CTF competition models based on AI, discover the characteristics and application areas of emerging technologies, solve some new problems arising therefrom, and put forward corresponding suggestions.

2. Background of cyberspace attack-with-defense drills

2.1. The current scale of global network assets

According to the bluebook "World Internet Development Report 2020" released at the 7th World Internet Conference held in Wuzhen, Zhejiang from November 23 to 24, 2020: In 2020, the number of Internet users in the world is about 4.54 billion, with a penetration rate of 59%, in 2023 and 2025, the global industrial Internet platform market size will grow to US $13.8 billion and US $19.9 billion respectively; In 2021, at the 8th World Internet Conference in Wuzhen, Zhejiang, the China Academy of Cyberspace released the "World Internet Development Report 2021", the report pointed out that as of June 2020 (May 31), the number of global Internet users reached 4.648 billion, accounting for 59.6% of the world's population; By the end of 2020, the number of global fixed broadband connections was 1.18 billion.

Table 1: Statistics of Internet Users in Major Countries in the World in 2020

Country	Number of Internet users (Unit:10000)	Internet penetration (%)	User growth rate (%)
China	90400	64.5	4018
India	56032	40.3	11210
America	31332	95.0	333
Indonesia	17127	62.7	8559
Brazil	14906	70.1	2980
Japan	11888	93.1	252
Russia	11642	80.1	3750
Mexico	8800	66.5	3145
Germany	7911	94.4	339

ISSN: 2664-9640

With such a huge number of users and assets, how to protect the confidentiality, integrity, and availability of information systems from being attacked by attackers is the top priority when considering cyberspace security issues during attack-with-defense drills.

2.2. Traditional and Emerging Cybersecurity Issues

2.2.1. Traditional cyberspace security defense means are single and passive

Traditional topological border defense devices, such as IDS, IPS, WAF, EPP, etc, or replacement and substitution ciphers are formed using the concepts of obfuscation and diffusion, called "previous generation defense technology". Several traditional attack methods spawned by it: SQL (Structured Query Language) injection attacks against classic databases such as MySQL, Oracle, Sybase, SQL Server, and DB2, CSS (XSS) cross-site script attack by using JavaScript website design flaws, chosen-ciphertext attack, known-plaintext attack, and ciphertext only attack based on traditional cryptography, etc. These constitute the previous generation of cyberspace security attacks and defense systems together.

Choosing a specific case, WAF (Web Application Firewall), a web application protection system, also known as the website application-level intrusion prevention system, is usually deployed at the edge of the network topology as the first line of defense for web applications. The most traditional WAF are hardware WAF based on transparent bridge mode, bypass mode, or reverse proxy mode and software WAF for request detection and blocking in the form of listening port or web container expansion. After the development of cloud technology, cloud WAF that adopts the principle of reverse proxy technology and virtual host technology appeared. However, the above traditional WAF is inseparable from the black and white list matching filtering mechanism, rule-based and exception-based protection mechanism in the context of regularization. Here, a piece of PHP code is used to simulate the WAF blacklist filtering mechanism:

```
<?php
  highlight_file("index.php");
  $abc = $_GET['select'];
  function abc($str)
  {
    if(preg_match('/select/',$res)){
      $res = str_replace('select','',$res);
    }
    return $res;
  }
  if(isset($_GET['select'])){
    if(abc($abc) == 'select123'){
      echo "right!";
    }else{
      echo "don't hack!";
    }
  }
?>
```

The user submits the parameter "abc" in the GET method on the client-side, and the value is "select123" to the backend for verification. However, if the string "select" appears in the value

ISSN: 2664-9640

and is matched by the regular matching function preg_match(), the str_replace() function will be called to filter and replace it, preventing attackers from constructing joint query injection and other malicious SQL statements to attack. At this time, the attacker will try to bypass the regular matching filter, such as using the "SELECT" to construct new attack statements, so the WAF manufacturer will add new rules:

```
if(preg_match('/select/i',$res)){
        $res = str_replace('select','',$res);
    }
```

"i" stands for case insensitivity, preventing attackers from exploiting case bypass. However, a new bypass pose will follow, Such as based on the principle of only one match of regular matching, use double-write ("selectselect") bypass, use string concatenation ($a=se, $b=lect, ab), etc. At this time, new WAF rules will be added for defense again. In the game between the two, constantly supplement and improve the WAF filtering rules, and build the most common defense system of current cyberspace security. However, this kind of traditional defense is often extremely passive.

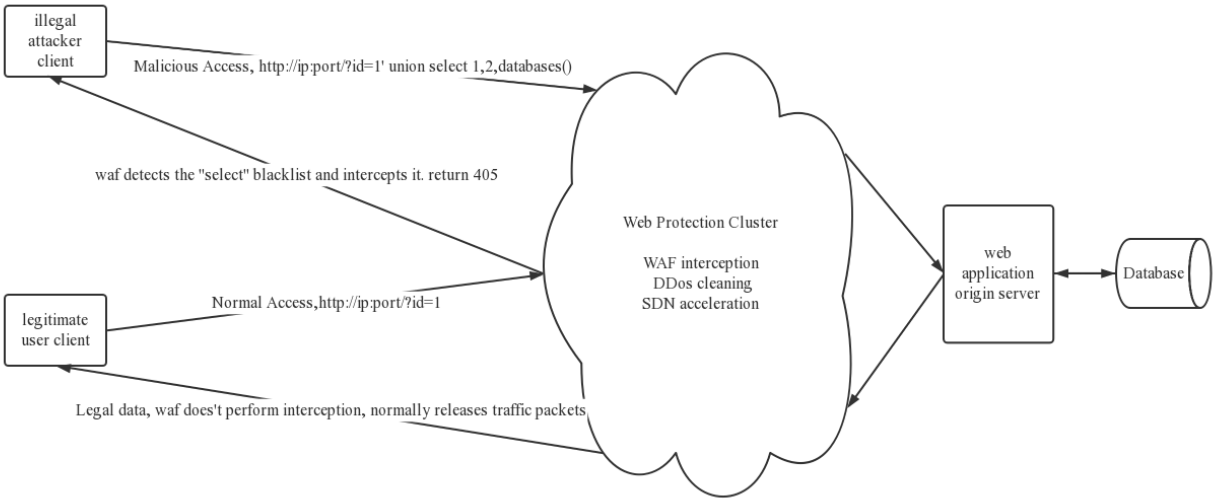

Figure 1: Schematic diagram of traditional WAF intercepting SQL injection

2.2.2. Emerging problems of cyberspace security under AI technology are prominent

Based on AI technology, autonomous and large-scale network attacks have been gradually formed. For example, for the availability, confidentiality, integrity, reliability, and undeniability of Cyberspace Security, using AI to identify patterns in big data, mining analysis of big data, and analysis of decision tree models to intrude on specific data assets or using machine learning to dig deep, grow and form a massive Mirai botnet powered by next-generation malware[3], as controlled terminals, these botnets consume a large amount of bandwidth and computing resources of the target by sending flooding application requests to the designated server, causing the target server to stop normal services. If the target is located in the SDN architecture, when the bandwidth is exhausted, other servers on the same link will also be affected. This is a new DDoS attack against the SDN itself based on AI technology. In addition, there are Packet-In flood attacks against the controller-centric architecture[4], overflow attacks against the switch's flow table[5], slow DoS attacks against the flow table timers[6], and CrossPath against the southbound channel attack[7], etc.

ISSN: 2664-9640

The traditional SQL injection attack mentioned above is often implemented through the attacker's manual injection or the injection attack tool based on Python language such as sqlmap. In the AI era, the traditional SQL injection attack methods are weak, so an autonomous SQL injection attack based on machine learning was born. Using the PHP code test sample proposed by STIVALET[8] as the original data set for machine learning, collecting a large number of web application source codes with 0-day vulnerabilities on the Internet as data sets for machine learning, and using the Skit-learn module in Python to complete autonomous SQL injection attacks[9].

Therefore, countries around the world gradually attach importance to and develop cyber attack-with-defense drills and CTF competitions, through this approach, the most realistic cyberspace attacks and defenses are simulated. How to use AI technology to develop the defense system for next-generation cyberspace security drills and prevent new types of cyber attacks that are also based on AI technology is particularly important.

3. Application of AI technology in Cyberspace Security

3.1. Traffic analysis technology based on autonomous identification

While AI technology optimizes attackers' attack methods, it is also upgrading and evolving the cyberspace security defense system. Such as traffic analysis technology based on autonomous identification, machine learning-based approach to detect malicious mobile software in Android apps (Androidtect), new worm virus recognition technology based on neural network technology, network security reasoning and evaluation system based on expert system technology, and antivirus infection system based on artificial immune technology[10], etc. Among them, the traffic analysis technology based on autonomous identification plays a pivotal role in the attack-with-defense drills and CTF competitions under the background of the current massive network traffic.

3.1.1. The technology's background in the birth

Benefiting from the development of hardware foundations such as single multimode optical fiber, 10-gigabit high-speed links, 100-gigabit Ethernet, and the emergence of next-generation communication technologies such as 5G, the traffic generated in the network is increasing geometrically. In 2021, China's mobile Internet access traffic will reach 221.6 billion GB, an increase of 33.9% over 2020. The average monthly flow of Internet users (DOU) in the whole year reached 13.49GB/household-month, an increase of 29.8% over 2020.

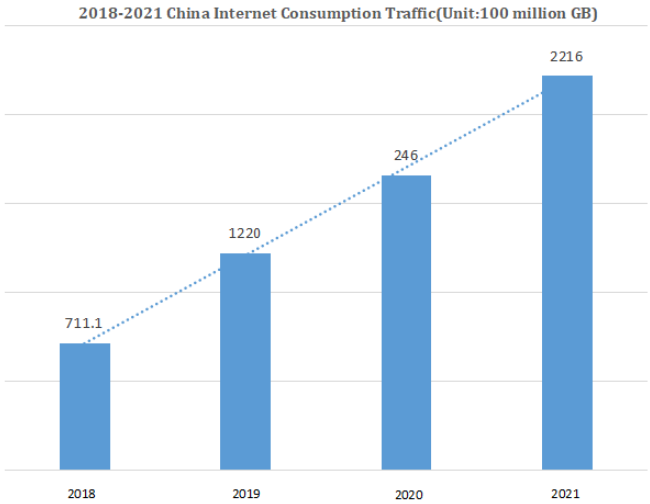

Figure 2: 2018-2021 China Internet Consumption Traffic Trend Bar Chart

ISSN: 2664-9640

With such a huge amount of traffic, in addition to normal website access traffic, known applications, and other APP traffic, there must be a lot of malicious attack traffic. Traditional malicious traffic monitoring and identification methods are usually traffic encryption and decryption technologies based on cryptography and fine-grained algorithms, passive traffic feature detection technology based on port and payload, and traffic analysis prediction technology by polling devices and capturing data link layer data, etc. Of course, there are also classic traffic identification systems such as intrusion detection and defense (IDS/IPS), and network management. However, in the face of large-scale traffic, the above traditional detection and identification systems are more or less weak, problems such as polling devices running out of bandwidth, and a huge amount of traffic being encrypted, the system cannot accurately identify malicious traffic appear.

3.1.2. Key points for this next-generation technology

Therefore, new network malicious traffic detection methods have become an urgent need in the field of cyberspace security, various new-generation traffic autonomous identification and analysis technologies based on deep learning emerge as the times require, and are put into the attack-with-defense drills. The key technical point lies in the AI foundation that relies on the convolutional neural network to convert traffic data packets into images that the system can recognize, at the same time, DNS data query is used to model the results, finally, it is matched with image fine-grained algorithm, cryptographic encryption, and decryption algorithm, etc. Realizing all-around active detection of malicious traffic in the network, identify and defend in advance. It makes up for the shortcomings of traffic detection technology and improves the security and confidentiality of the computer network system.

3.2. Machine learning-based approach to detect malicious mobile software in Android apps

3.2.1. Definition of Malicious Program

Malicious programs usually refer to a piece of code program that is aggressive, self-replicating, host-dependent, or with malicious intentions of the attacker, common malicious programs include Trojan horses, worms viruses, etc. It is often hidden and embedded in a legal program, implanted into the host computer through the exposed interface of the computer network and system, and triggered to execute at a specific time or under specific conditions, to achieve the purpose of destroying the information system and files and stealing user information. This kind of attack method is simple, but the harm and impact it brings to computer users are huge, so it is very common in cyberspace attack-with-defense drills.

3.2.2. AI-based malicious program detection technology - Androidetect

Traditional tools and methods for detecting malicious programs are very simple and inflexible, and most of them can only detect the existence of malicious programs or can not detect instantaneous attacks. In this context, some program detection technologies based on AI such as machine learning have been born. Among them, the typical representative is Androidetect, which is an Android malicious application detection technology based on machine learning proposed by Linfeng Wei, Weiqi Luo, Jian Wang, Yanjun Zhong, Xiaoqian zhang1, Zheng Yan, and others, this technology is proposed after combining and perfecting the applications of Sanz et al use machine learning in the static analysis, such as an Android malicious application detection method based on application permission and an Enclamald classifier detection method based on contrast correction mode, which can be used to detect the existence of malicious applications. The system uses process injection technology, hook technology, and inter-process communication to extract the features of Android applications to construct feature vectors, and takes this feature vector as its machine learning training classifier. At the same time, a judgment algorithm of application function class is designed to establish the

ISSN: 2664-9640

distinction and classification between normal applications and malicious applications, then, two common machine learning algorithms, naive Bayes and decision tree are used to train and test the training classifier, finally, through the designed system log function partition (log access module and log analysis module), the inspection and identification of the security threat feature points of malicious programs are completed[11]. In this way, by using AI technology such as machine learning and analyzing system functions and sensitive system interfaces, we have completed the detection of transient attacks that many malware detection tools could not complete before, optimized the computer's identification accuracy for malicious programs, and greatly improved the security of the user's computer, this makes it possible for defenders to respond well to malicious programs in both attack-with-defense drills and actual combat.

3.3. Emerging AI technology breaks through traditional attack-with-defense drills

3.3.1. The birth of cyber attack-with-defense drills

Today's cyberspace security is facing a severe ecological environment, which leads to an invisible threat to the construction of the country's key information infrastructure. In 2016, The Ministry of Public Security of the People's Republic of China, together with the Civil Aviation Administration of China, State Grid Corporation of China, and other units, launched the first cybersecurity attack-with-defense drill, called "Network Protection 2016". At the same time, the "The Cybersecurity Law of the People's Republic of China" was promulgated, and relevant provisions on cyber security drills: the operators of key information infrastructure should "develop contingency plans for cybersecurity incidents and conduct regular drills". Then for the 2022 Beijing Winter Olympics Games and Winter Paralympics Games, a special cyberspace security team was set up to protect key projects. Since then, as one of the important job responsibilities of cyberspace security practitioners, it has also become an important part of cyberspace security construction, the term "network protection project" has entered people's vision. The traditional network protection project usually divides the government, public institutions, enterprises, and financial institutions into "red and blue teams", that is, the attacker and the defender, through actual network attack and defense (including network attack and physical attack), the security personnel of these units finds potential network threats and system security vulnerabilities by colliding with the "spear" and "shield" without affecting target's information system the availability of confidentiality and integrity, timely notification, timely warning, timely response, and timely repair, it greatly improved the information security level of some key units.

3.3.2. Disadvantages of traditional attack-with-defense drills

The traditional attack-with-defense drills still have their limitations, because there are too many human factors affecting the offensive and defensive drills, the main ones are the relevant security personnel of the unit and the decision-making of the responsible leaders. When relevant security personnel conducts penetration testing, they may have certain human biases in combination with their interests or their technical level, they may carefully penetrate one system but ignore other systems, which will weaken the vulnerability of the information system and create the illusion of less threat. As an important influencing factor of the "information system security assessment", the decision-making in charge of leadership may also resist the attack-with-defense drill due to the excessive expenditure of participating in the attack-with-defense drill, fear of affecting the normal operation of core business systems, etc., resulting in poor drill results and failure to play its due role.

Also, the form of the traditional attack-with-defense drill is single and passive. The drill is carried out through traditional steps such as collecting information in the early stage, the discovery of possible threats and vulnerabilities, formal penetration of threats and vulnerabilities, confirmation of the existence and harm of vulnerabilities, formation of reports

ISSN: 2664-9640

for notification, the emergency response of the involved units, repairing vulnerabilities and completing the drill. So, the threats and vulnerabilities discovered are not comprehensive and have a certain one-sidedness. The passivity is because of the one-sided threats and loopholes discovered by its security personnel, and only passive one-sided repairs can be carried out accordingly. This kind of repair is not complete, especially when various applications and systems are nested and interrelated with each other, such limited cyberspace attack-with-defense drills often do not work well.

3.3.3. Attack-with-defense drills in the context of emerging AI

Attack-with-defense drills based on AI technology are gradually emerging. Cyber BattleSim, Microsoft's open-source AI attack-with-defense training platform, whose Python-based Open AI Gym interface allows the use of reinforcement learning algorithms to train automated agents, with fixed network topology and agents, the simulation environment can be parameterized by exploiting a set of vulnerabilities that move horizontally in the network. It simulates the high-level abstraction of computer network and cyberspace security concept, to achieve the purpose of the attack-with-defense drill of independent attack, and effectively reduce the influence of human factors on penetration testers.

Then, take the "Network Security Brain" developed by 360 Group as an example. It uses deep learning technology combined with big data technology to form network probes, collects a large number of network security program behavior big data, and then detects and evaluates the vulnerabilities of all systems in the huge network system, and ranks them from high to low according to the hazard level. The possible security vulnerabilities or threats are reported in turn and then delivered to security personnel for reference reproduction and confirmation. In this way, the breadth and depth of information system security detection can be unified and comprehensively covered, avoid the one-sided penetration detection of a single system in traditional attack-with-defense drills, and also reduce the excessive interference of human factors to a certain extent. So that the network protection project can reflect a better effect.

Similarly, Baidu Security integrates "Baidu Brain" and cloud security interconnection technology, and has also developed its own AI attack-with-defense drills tool: the intelligent threat hunting platform. Relying on autonomous traffic analysis technology, anomaly detection models, and intelligent algorithms, the platform introduces a series of AI security capabilities including intelligent tagging technology, UEBA potential attacker detection, and intelligent traceability, it realizes three core security functions: detection and early warning of 0day vulnerability attack, early detection of potential attackers and accurate traceability afterward, greatly reduces the cost of security operation and maintenance and cyberspace attack-with-defense drills, and provides more valuable data to support advanced threat analysis and decision-making.

It can be seen that with the emphasis on cyberspace security, the "network protection project" based on AI technology has gradually become one of the important layouts for countries to deal with cyberspace security issues.

4. AI-based CTF cybersecurity competition

4.1. Traditional CTF competition mode

CTF (Capture The Flag) cybersecurity competition started at the DEFCON Global Hacker Conference in 1996. It was originally an important platform for security technicians and security enthusiasts to exchange security technologies. In today's increasingly severe cyberspace security environment, relying on the competition mode of replacing battle with competition and promoting learning with practice, has gradually become one of the important ways for countries around the world to cultivate and discover cyberspace security talents, and

ISSN: 2664-9640

popularize basic knowledge of cyberspace security. The traditional CTF competition is mainly divided into Web (Web Security), Pwn (Binary Security), Misc (Miscellaneous Research), Reverse (Software Reverse), Crypto (Cryptography) five directions. Through various technical means, the safety technicians find the flag file from the five directions and submit it to the organizer to obtain the scores in the arena. The flag file may come from a remote server, a complex software, or it may be hidden in a piece of data encrypted by a cryptographic algorithm, or a group of network device traffic and audio and video files[12].

4.2. Emerging CTF Competition Directions

In the more than 20 years of CTF development, according to the technological trends of the times, BC—BlockChain, AWD—Attack With Defence, IN—internal network, TC—Trusted Computing, IOT—Internet of Things, Real SRC—Security Response Center have been extended. These directions are more realistic and closer to the actual combat of the competition.

4.3. CTF questions with AI as the test point

With the development of AI, the CTF cybersecurity competition based on AI technology has also been born. In 2018, JD Security joined hands with Kansue Academy, a domestic security talent Huangpu Military Academy under Shanghai Kansue Technology Co., Ltd., to hold a two-month "Kanxue" CTF cybersecurity competition, attracting nearly 40,000 White Hats and safety enthusiasts attend. The biggest focus of this competition is an AI CTF question designed by the JD Secururity Response Center have been extended. These directions are more realistic and closer to the actual combat of it Silicon Valley R&D Center team. This is the first time that deep learning, an AI technology in the field of AI, has appeared in the CTF competition as a test point. The design idea of this problem is to find the logic flaws and vulnerabilities in the algorithm code on the basis that the solver can understand its deep learning algorithm, and then complete the repair and patch after adding, deleting, and modifying the algorithm code. According to the description of the problem-making team, the difficulty of the problem has been reduced, and the participants are only required to find and correct a specific deep learning algorithm error, the purpose of this design is that in the real cyberspace attack-with-defense confrontation, the algorithm of modifying the deep learning model on a large scale will consume a lot of time and energy, which is impractical in practice. However, there are still a lot of things that contestants need to consider in this question. First, the contestants need to understand the basic logic of the deep learning algorithm, find out the existing errors, and correct the errors without affecting the deep learning algorithm's judgment of the target sample. This topic is a good reflection of the real attack and defense, under the influence of AI technology, the attacker occupies the active position, but the defender is in a passive state for a long time. According to the statistics data after the game, a total of 1,500 people participated in the answer to this question, but only 2 people solved it in the end. Therefore, the appearance of the AI CTF question can be regarded as an exploration to change this unbalanced state.

4.4. CTF innovation track under AI technology

In the same year, at the BlackHat Europe conference, the Baidu security research team proposed and realized that an object can "disappear" in a deep learning system sample, thereby bypassing AI's discovery and recognition of the object. Inspired by this technology, in the autonomous driving CTF competition in September, the organizer launched a challenge, the title of the competition - "Invisibility Cloak". That is, through 3D simulation games to simulate the AI perception attack of autonomous driving in the physical world, the participating teams can experience and challenge in near-real autonomous driving scenarios. The organizer will inform the participating teams of the open-source universal object recognition model in advance before the competition, in the normal AI safety mode, the automatic driving vehicle identifies the obstacles ahead through the machine learning samples of the model, and

ISSN: 2664-9640

automatically brakes or detours to ensure driving safety, the participating teams need to discover the vulnerabilities in the model. According to the regulations of the topic, they will use AI confrontation machine learning technology to make the obstacles "disappear" from the sample library of the learning system, so that the automatic driving vehicle cannot identify the obstacles in front, and thus get the scores by collision. The difficulty of this competition is that in a dynamic environment, the model will continue to collect samples, compared with simple AI spoofing of static pictures, the forgery of a single or a few static frames cannot achieve the purpose of confronting machine learning, in addition, there are a large number of sensors in the automatic driving vehicle, and multiple technologies are used for object recognition and sample collection, Therefore, it can defend against multiple attacks. It is necessary to require a clear division of labor and full cooperation between the participating teams to complete the competition.

It can be seen that starting from a CTF question with AI technology as the test point for a specific topic in a specific direction, and gradually forming a CTF competition with AI security as a separate track, deepening the application of AI technology in CTF competition from point to area is an inevitable development trend in the field of cyberspace security.

5. 5. Conclusion

Today, when AI technology is in the ascendant, it will inevitably lead to major changes in all fields of society, including the field of cyberspace security. This article starts from the era background and technical background of cyberspace security attack-with-defense drills; with the application of some emerging AI technologies in cyberspace security, AI technologies break through the traditional attack-with-defense drills during network protection projects. At last, the article discusses the current CTF competitions based on AI. It shows that the development of AI provides more attack methods for the attacker, while causing more potential threats to cyberspace security, it also gives security researchers more ways to solve security problems and improve system security. "Without cybersecurity, there is no national security", today's cyberspace security already exists as a national strategic level demand. The far-reaching impact and transformation of AI technology on it will surely become the core of research and discussion among many scholars and experts. This paper provides many examples to demonstrate that AI technology is a "double-edged sword" in the field of cyberspace security, and discusses the deep integration of AI and attack-with-defense drills and CTF competitions. Therefore, this paper proposes to apply AI technology more widely in attack-with-defense drills such as net protection operations and CTF competitions. In this way, it can help security personnel to contact the attack and defense of AI technology in daily training, building an emerging cyberspace security attack and defense system, effectively avoiding the large-scale impact of AI attacks in actual combat, and greatly improving system security. At the same time, we hope that it can provide a reference for the research discussions of other scholars and experts.

Acknowledgments

The study is funded in part by a research grant from the Science and Technology Council of Nanchong City (SXQHJH051).

References

[1] Feng Lin. Automatic generation of DNS stealing data for AI model training [J]. Journal of Information Security, 2021, (1): 1-16.

ISSN: 2664-9640

[2] The U.S. and China lead the world in Internet development - Release of the Blue Books of "World Internet Development Report 2020" and "China Internet Development Report 2020" [J]. Informatization Construction, 2020, (12):32-34.

[3] Information Security in 2020: The Widespread Emergence of Artificial Intelligence (AI) in Various Information Security Systems [R]. 2019.11.06.

[4] Rajat Kandoi,Markku Antikainen.Denial-of-service attacks in OpenFlow SDN networks[C]. Integrated Network Management(IM),2015:1322-1326.

[5] Xu J F, Wang L M, Xu Z.Survey on Resource Consumption Attacks and Defenses in Software-Defined Networking[J].Journal of Cyber Security,2020,5(04):72-95.

[6] Jiahao Cao, Qi Li, Renjie Xie, et al.The CrossPath Attack: Disrupting the SDN Control Channel via Shared Links[C].USENIX Security Symposium,2019:19-36

[7] STIVALET B, FONG E. Large Scale Generation of Complex and Faulty PHP Test Cases[C]. IEEE. 2016 IEEE International Conference on Software Testing, Verification and Validation(ICST), April 11-15, 2016, Chicago, IL, USA. New York: IEEE, 2016: 409-415.

[8] Hu Jianwei, Zhao Wei, Yan Zheng, et al. Analysis and implementation of machine learning-based SQL injection vulnerability mining technology [J]. Information Network Security, 2019, 19(11): 36-4.

[9] Guo Chun, Cai Wenyan, Shen Guowei, et al. SQL injection attack detection method based on key payload interception [J]. Information Network Security, 2021, 21(7): 43-53.

[10] Jiao Shaobo, Shen Hao, Chen Xin. Exploring the application of artificial intelligence technology in cyberspace security defense[J]. Network Security Technology and Application, 2021,(2):176-178.

[11] Wei, LF (Wei, Linfeng) 1; Luo, WQ (Luo, Weiqi) 1; Weng, J (Weng, Jian) 1; Zhong, YJ (Zhong, Yanjun) 1; Zhang, XQ (zhang, Xiaoqian) 1; Yan, Z (Yan, Zheng) 2. Machine Learning-Based Malicious Application Detection of Android [J].IEEE ACCESS,2017,Vol.5,25591-25601.

[12] Jiang Kaida, Wu Yongxing (Shanghai Jiaotong University). Network Security Competition: Opening a Channel for Training Security Talents [J]. "China Education Network", 2019, (9): 52-53.