Winter 1-15-2019

The Benefits of Artificial Intelligence in Cybersecurity

Ricardo Calderon
La Salle University, calderonr1@student.lasalle.edu

The Benefits of Artificial Intelligence in Cybersecurity

Ricardo Calderon

La Salle University

Abstract

cyberthreats have increased extensively during the last decade. Cybercriminals have become more sophisticated. Current security controls are not enough to defend networks from the number of highly skilled cybercriminals. Cybercriminals have learned how to evade the most sophisticated tools, such as Intrusion Detection and Prevention Systems (IDPS), and botnets are almost invisible to current tools. Fortunately, the application of Artificial Intelligence (AI) may increase the detection rate of IDPS systems, and Machine Learning (ML) techniques are able to mine data to detect botnets' sources. However, the implementation of AI may bring other risks, and cybersecurity experts need to find a balance between risk and benefits.

Keywords: Cybersecurity, artificial intelligence, machine learning, deep learning, deep belief network, IDPS, botnet

Introduction

Everybody is at risk for a cyberattack. According to Myriam Dunn Cavelty (2018), cybersecurity "…refers to the set of activities and measures, technical and non-technical, intended to protect the 'real geography' of cyberspace but also devices, software, and the information they contain and communicate, from all possible threats" (Cavelty 2010). As technology advances every day, cybercriminals are becoming more sophisticated and getting ahead of current cybersecurity controls. In order to get ahead of cybercriminals, experts are beginning to use Artificial Intelligence (AI) to counter new cyberattacks (Harel, Gal, and Elovici, 2017). AI is a discipline in computer science that uses complex mathematical algorithms to imitate human thinking (Lidestri 2018). The term Artificial Intelligence was proposed in 1956 by John McCarthy and other researchers. The first steps in AI achieved games such as the checkers game that was able to learn through training. The game was capable of playing better than an average player. As it was the end of the first decade for AI, the achievement was a great step in digital computing. The problem was how to apply AI to solve real-world problems. The researchers lacked a vast amount of knowledge which prevented them from understanding the problems (Tecuci, 2011). Although real AI has not been achieved yet, it has grown at a faster pace and has revolutionized various fields and industries including automotive, medicine, and astronomy. The increased demand to stop cyberattacks led to the application of AI-based techniques in cybersecurity.

AI has multiple branches or subsets. One AI-based technique is Machine Learning (ML). Machine Learning is a subset of AI that teaches machines how to make decisions (Feizollah, Anuar, Salleh, Amalina, & Shamshirband 2013). The growth of ML has helped researchers to

develop techniques to detect tumors, and enhance cybersecurity techniques to detect malware in networks and phishing emails.

Another branch of AI is Deep Learning (DL) which researchers describe as a type of ML that performs pattern recognition and predictions (Polson, 2017). DL is capable of handling humongous datasets. This allows its application in a large array of fields such as image rendering, stock market prediction, and agriculture. DL improves areas of cybersecurity such as intrusion detection and botnet detection due to the high processing power that it has to examine data and learn from experience.

The goal of this paper is to inform readers about the possibilities of using AI in cybersecurity by showing both the benefits and the risks. Cybersecurity experts are using ML and DL to solve problems in the areas of Botnet Detection, and Intrusion Detection and Prevention Systems (IDPS). However, the integration of AI-based technologies in organizations may have implications which cybersecurity experts need to address to ensure cyber safety. AI may also impact technology consumers who are using devices that, in one way or another, are already using the technology.

Cybersecurity problems that AI can solve

With technological advancements in the cyberspace, cybersecurity faces new problems. Some problems have existed for decades but cybersecurity experts need to find new ways to defend networks from existing problems. Two of the existing problems are botnets, that are used to launch Distributed Denial of Service (DDoS) attacks, and IDPS that generate large numbers of false alarms which distract cybersecurity experts from finding real threats.

A botnet is a network of computers and other devices which are referred to as bots. Computers that are part of a botnet connect to it by malware infection. After the infection in

launched, a “botmaster” sends commands to the bots via a network channel. Usually the botmaster encrypts the channel to avoid detection. The botmaster uses a Command and a Control (C&C) server to push commands and patches. Botnets play a major role in DDoS attacks. In fact, the larger the botnet, the more effective the DDoS attack will be. Additionally, botnets are also used for identity theft and stealing data (Mathur, Raheja, & Ahlawat 2018). In 2016, the Mirai malware infected Internet of Things (IoT) devices and created a botnet that connected approximately 500,000 IoT devices together. The botnet was used to unleash devastating DDoS attacks on sites and services (De Donno, Dragoni, Giaretta, and Spognardi 2018). In addition, Mirai malware is open-source, which means that other cybercriminals may add new features to the malware, and create new variations of Mirai. AI has the capability to detect botnets inside networks. The detection of botnets will help prevent the infection of more devices and stop DDoS attacks, and data leakage.

An IDPS is a technology that network and system administrators use to detect intrusions. After the IDPS detects intrusion, the authorized administrators may receive email alerts. This technology not only detects intrusions but also prevents intrusions when an attacker tries to gain unauthorized access to a network (Whitman and Mattord 2017). To achieve a higher security level, network administrators need to properly configure IDPS tools. Developers have created hardware and software-based Intrusion Detection and Prevention Systems. Network administrators may install a system on a host, which they call Host-based IDPS, or on the network, which they refer to as Network-based IDPS. One of the main problems is setting up and configuring an IDPS is time-consuming because a standard configuration does not exist. Network traffic differs organizations. Due to that, IDPSs generate a large number of false alerts

or “false positives.” With AI, cybersecurity and network administrators hope to filter out false alarms and increase detections rate.

Intrusion Detection and Intrusion Prevention

IDPS systems come in two categories. Intrusion Detection System (IDS), and Intrusion Prevention System (IPS). Currently, IDPS technology relies on Signature-based and on Anomaly-based systems. Signature-based detection systems rely on databases of known threats to detect intrusions. Signature-based systems examine incoming packets and retrieve the signatures from network packets and compare them against the database. If there is a match, the system assumes that an intrusion has been detected. It is an effective method to detect intrusions that have been previously detected, but one of the major problems is that it only works against threats that it knows (Jean-Philippe 2018). For example, after Mirai botnet spread, developers created patches to protect IoT devices from the malware. In the process, a signature was identified for Mira. If an attacker attempts to infect a patched IoT device the signature-based system will prevent it. However, a signature-based system cannot detect a variation of Mirai because the signature differs from the database.

On the other hand, there are anomaly-based detection systems. Unlike signature-based detection systems, anomaly-based detection systems signal intrusions or attempts by assessing the behavior in a network. For example, if a new malware makes its way into a network, the signature-based detection system would not categorize that malware as legitimate whereas the anomaly-based detection system will analyze its behavior and determine whether it is a threat. Detecting threats because of the behavior rather than by the signatures indicates that the anomaly-based detection system is more efficient because it does not need previous information about the incoming threat. In order to detect new threats, researchers and administrators need to

create protocols within the system which will function as validators. Those protocols determine what normal or legitimate network traffic resembles (Jose, Malathi, Reddy, and Jayaseeli 2018). The anomaly-based systems rely on human interaction to have new rules. They cannot find the threat if the rule that detects it does not exist.

Machine Learning Approach

As cybercriminals become more sophisticated, cybersecurity experts need more sophisticated tools and techniques to be able to defend their networks. ML-based IDPS may enhance defenses and at the same time reduce false positives. There are six different types of Machine Learning methods, and each one has unique characteristics and values that cybersecurity experts may benefit from. According to Ruth Jean- Philippe (2018), all ML methods are not alike, therefore, researchers need to provide the correct data for the ML-based system to work to its fullest. Among the six ML methods, two of them are outstanding for cybersecurity.

The first method is Artificial Neural Networks (ANN). ANN are nodes that imitate the human brain. This method uses processing nodes or neurons that connect to each other, and also connect to a hidden layer (Jean-Phillipe, 2018). According to Jean-Phillipe's research, ANNs are capable of recognizing patterns that are very complex for humans to recognize. Also, ANNs are able to recognize unprecise patterns. The application of ANN in IDPS enhances network security. Cybercriminals have learned to evade security controls. They are capable of deploying attacks that do not trigger alerts in the system which makes their detection a harder task for cybersecurity experts. For example, if cybercriminals perform a port scan, passively, this mimics a legitimate connection in order to detect open ports. However, ANN would be capable of detecting when a connection is legitimate and when it should trigger a security alert due to the

connection patterns. Usually, passive scans start a connection and then closes them before the connection reaches the end and thing would be detected as malicious.

The second ML method is Genetic Algorithm (GA). GA detects threats by learning from experience given to previous anomaly behavior. Similar to the human brain, humans know that fire is dangerous because of the experience of ancestors. GA is useful to detect common threats with common patterns. So, GA uses the previous patterns to make decisions on new patterns that the system cannot recognize (Jean-Phillipe, 2018). Applying this method to ML-based IDPS systems, researchers would be able to increase detection rates for new anomalies. For example, if a ransomware manages to penetrate the firewall, via email or other vector, when it intends to spread and encrypt files, the ML-based IDPS using GA will detect it and prevent the encryption of a large cluster of devices across the network.

Unlike signature-based systems, ML-based systems do not need databases with signatures (Jean-Philippe, 2018). Feeding supervised machine learning algorithms with a dataset which contains information about what normal network traffic should look like and providing a whitelist that the ML-based IDPS will use to detect threats. The ML-based IDPS system can make decisions against different new patterns. Regular IDPSs do not have these capabilities as they rely on previous configurations to protect networks.

Deep Learning Approach

In attempt to increase detection accuracy, other methods have been proposed. Deep Learning is a branch of ML with a higher level of complexity. Researchers define DL as a neural network that contains at least three hidden layers as *Figure 1* demonstrates (Roosmalen, Vranken, & Eekelen, 2018). Researchers provide data in the input layer of the deep learning neural network.

The input layer then sends the data towards several hidden layers that perform algorithms to produce possible outputs.

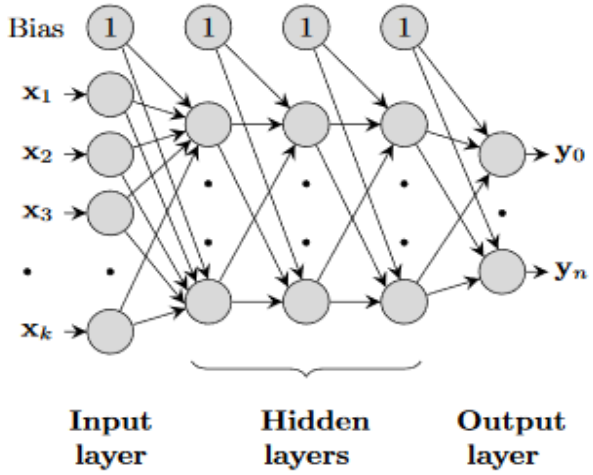

Figure 1: A deep learning neural network

(Roosmalen, Vranken, & Eekelen, 2018)

In 2006, Geoffrey Hinton proposed a data processing model which was named deep Belief Network (DBN). DBN has been successfully applied in areas such as speech and object recognition. DBN is capable of processing large amount of data which makes it effective for DL-based intrusion detection tools. Researchers from CRRC Qingdao Sifang co., LTD carried out studies to determine the impact DBN had on intrusion detection (Qu, Zhang, Shao, & Qi, 2017). They divided their intrusion detection model in two steps: The first step trains the Restricted Boltzmann Machine (RBM) which is the foundation of DBN and is a hidden layer that has a connection with a visible layer. RBM benefits DBN because it uses large a number of visual and hidden layers. This allows DBN to process more data that it then sends to the second step, which is the Back Propagation (BP) neural network. The second step adds BP neural network, which receives the data from the previous step and monitors the network (Qu, Zhang, Shao, & Qi,

2017). BP is the last layer in a DBN which decides and attempts to identify false positives and discards them in order to provide a more accurate result.

Qu, Zhang, Shao, and Qi (2017) have proposed an IDS that integrates with DBN to detect threats. In their model, when the IDS scans the network, the DBN receives the raw data that the IDS has produced. The DBN processes the data and estimates the number of layers that it would need. Then it creates a training dataset to start the process in which the DBN uses that dataset to perform its calculations and determine if it is a false positive or a threat. Prior to determining if the data belongs to a threat, the DBN calculates the errors in addition to the results it expects. That process is a constant loop that stops when it obtains the results expected by DBN. *Figure 2* depicts the flow.

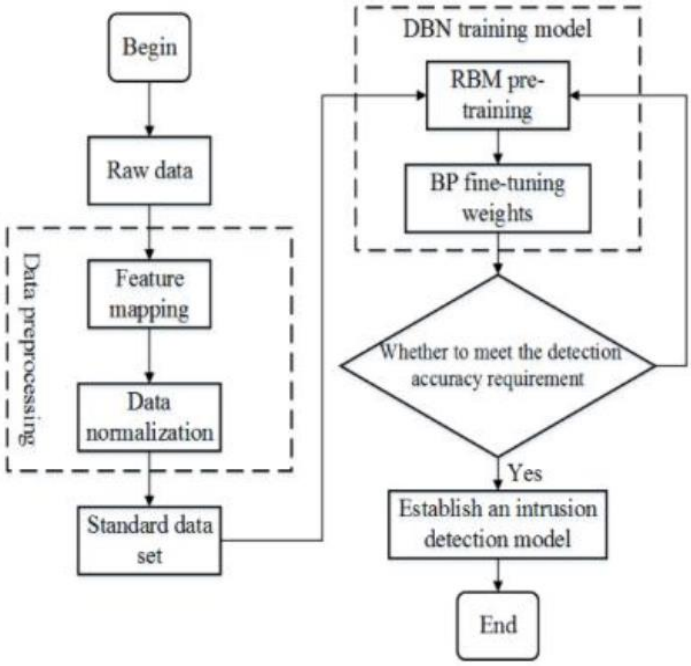

Figure 2: An intrusion detection model based on DBN.

(Qu, Zhang, Shao, & Qi, 2017).

A comparison with current intrusion detection systems, false positives are common. Researchers from CRRC Qingdao Sifang co., LTD (2017) concluded with the simulations they ran that the accuracy rate was 92.25%. The remaining 7.75% is a smaller window for false positives to exists. Often, when current IDS systems trigger alerts, cybersecurity experts need to spend valuable time to analyze the alert in order to determine whether it is a false positive. With DL methods, false positive rates will decrease which at the same time will increase performance and detection.

Botnet detection

Xuan Dau Hoang and Quyng Chi Nguyen (2018) describe a botnet as a changing environment. Bots are constantly sending lookup queries. The goal of the queries is to obtain the IP address of the Command and Control (C&C) server in the DNS system. C&C servers very often change DNS and IP addresses to avoid detection. Hoang and Nguyen proposed a two-phase detection model that uses machine learning algorithms to increase the possibilities of detecting botnets (Xuan and Nguyen 2018). *Figure 3* demonstrates the workflow of the botnet detection by using DNS queries by Hoang and Nguyen.

The first phase is the training or learning phase. The training phase uses a labeling and classification system. In this phase, the ML algorithm will collect data about the DNS queries from the bots in the botnet. During the training phase, the ML algorithm extracts the domain names from the queries for the training phase. The domain names belong to botmasters that control devices in the botnet. This is the pre-processing step. The ML system then uses the data from the pre-processing step for the training that it needs to undergo in order to learn the pattern and detect the botnet. The training produces classifiers and when the first phase reaches this point, it is ready to pass to the detection phase.

The second phase is the detection phase. The detection phase analyzes the results from the training phase. The analysis of the domain names produces a classifier that determines the legitimacy of the domain name. The classifier determines if the DNS queries are legitimate or belong to a botnet.

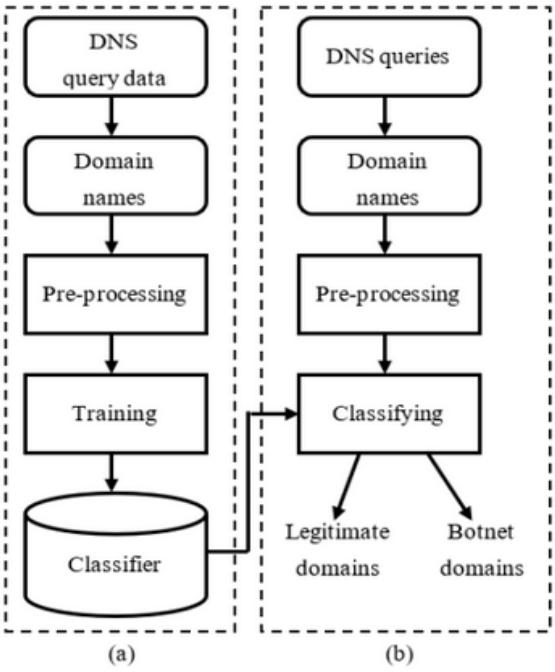

Figure 3: (a) is the training phase and (b) is the detection phase.

(Xuan and Nguyen 2018)

Aymen Awadi and Bahari Belaton (2015) proposed a similar multi-phased approach. Their approach relies heavily on an Intrusion Detection Systems to detect botnets. However, Awadi's and Belaton's phase one uses a signature-based database algorithm unlike Hoang's and Nguyen's; Awadi's and Belaton's phase two gathers data from the botnet and detects attacks that the botnet is launching whereas Hoang's and Nguyen's gathers botnet data in phase one and focuses on detection in phase two (Awadi, and Belaton 2015). Awadi's and Belaton's process is effective for attack detection, but, without the use of ML, it does not create data that it can use to detect IP address changes and seemingly legitimate behaviors.

Xuan and Nguyen demonstrated through experimentation the accuracy or their botnet detection model. They used common machine learning algorithms that function under supervision. Some of the algorithms that they used in their model were k-Nearest Neighbor (kNN), Random Forest (RF), Decision Trees (DT), and Naïve Bayes (NB). The tests provided impacting results, but the most outstanding algorithms they tested were kNN and RF (Xuan and Nguyen 2018). kNN algorithm was on average 90% accurate detecting botnets, and RF averaged 88% accuracy.

Machine Learning and Deep Learning Example

Companies such as Fortinet are applying machine learning and deep learning for threat detection systems. Fortinet users a Self-Evolving Detection System (SEDS) that uses both ML and DL to detect unknown threats. ML and DL train SEDS which improves its accuracy for threat detection. SEDS learn from the data that it accumulates, which allows it to detect a variety of threats such as intrusions, botnets, and malware. Fortinet's product requires humongous amounts of data for training, and not only that, it also requires some hardware capacity to function at its fullest. For training, SEDS involves training algorithms such as supervise and unsupervised learning (Fortinet). Due to its high capacity from enormous amounts of data, SEDS becomes more precise to detect threats. Fortinet claims that their product is capable of detecting zero-day threats. For organizations, this means that they will see vectors ahead of cybercriminals before they can exploit them. When organizations discover these vectors, they may be able to develop their own patches to cover the network holes.

The risks of using AI in cybersecurity

Although AI brings many benefits, the integration of AI in a work environment can bring risks that are more complex. "...the double-edged sword is that while AI systems can help defend

against cyberattacks, they also present new targets for hackers, potentially posing a number of new cybersecurity vulnerabilities for individuals and businesses," Zielezienski said (Chordas, 2017). Individuals are negatively impacted as well. Strong security measures by regular users makes them more vulnerable to attacks. Often, users are not aware of the security risks that they face when using new technologies (Chordas, 2017). Regular users often miss security patches for their devices. They tend to use and run applications without patches. As a result, unpatched applications run in the background and most of the time regular users do not use them.

With the widespread use of AI, information about AI become easily accessible by anyone. There are books that teach you how to program AI. Miles Brundage, Shahar Avin, Jack Clark, Helen Toner, Peter Eckersley, Ben Garfinkel, and other authors, including Hyrum Anderson claim that:

> Efforts to prevent malicious uses solely through limiting AI code proliferation are unlikely to succeed fully, both due to less-than-perfect compliance and because sufficiently motivated and well resourced actors can use espionage to obtain such code. However, the risk from less capable actors using AI can likely be reduced through a combination of interventions aimed at making systems more secure, responsibly disclosing developments that could be misused, and increasing threat awareness among policymakers (p. 59).

The establishment of regulations to reduce the widespread use of AI code is a complex task for policymakers. As resourceful cybercriminals learn how to use AI maliciously, they become a more prevalent threat.

In 2016, the Defense Advanced Research Projects Agency (DARPA) carried out a "bug hunting competition. The competition included Capture the Flag (CTF) games. CTF challenges

are useful in the hacker community since it allows them to learn new techniques. During the competition, seven team used automated AI tools that identified internal flaws and patched them. Since then, the Massachusetts Institute of Technology (MIT) researchers have used AI to detect threats and alerts security professionals to act (Wilner, 2018). The progressive advance of the AI usage in cybersecurity not only involves cybercriminals, it also involves nation-state actors. Nation-state actors will be able to exploit unknown vulnerabilities in a faster fashion and exfiltrate sensitive information that could contain information about power grids. They will leverage that information to use it against a nation. Artificial Intelligence itself will be a new weapon for cyberespionage.

Conclusion

Artificial Intelligence is a vast field that researchers and cybersecurity experts need to explore. They have applied AI and its branches in other areas that use technology for support. Research demonstrates that AI can be beneficial for cybersecurity. In Intrusion Detection and Prevention Systems research proves that Machine Learning is a technique that brings positive results. The application of ML in IDPS systems reduces false positive and increases accuracy and at the same time, learns to understand new threats. Similarly, Deep Learning is more powerful than ML for IDPS systems. DL research demonstrates that accuracy rate is higher when researchers used DL with Deep Belief Networks (DBN). With the help of DBN, IDPSs have more nodes to perform calculations and therefore produce better results.

Botnet detection also benefits from AI. Researchers used ML to learn techniques to detect botnets by analyzing domain queries that botmasters use to communicate with devices. The botnet detection with domain queries model uses two phases: the learning phase, in which ML-based system extracts the data to classify bad data and good data; and the detection phase, in

which in uses the data from the first phase to detect botnets. When botnet detection systems apply k-Nearest Neighbor and Random Forest results are accurate and reduce false positives. The application of AI in more areas such as cybersecurity would increase the attack surface or vectors of attack in an organization. AI tools may additionally add new vulnerabilities in systems. Cybercriminals will become more knowledgeable to develop new tools that use AI to exploit vulnerabilities. This would allow cybercriminals to hide their intentions when probing networks, and sending malware. Cybersecurity professionals will need vigorous policies to regulate AI in organizations so threats are less imminent.

Bibliography

1. Mathur, L., Raheja, M., & Ahlawat, P. (2018). Botnet detection via mining of network traffic flow. *Procedia Computer Science, 132*, 1668-1677. doi:10.1016/j.procs.2018.05.137

2. Xuan, D. H., & Nguyen, Q. C. (2018). Botnet detection based on machine learning techniques using DNS query data. *Future Internet, 10*(5), 43. doi:http://dbproxy.lasalle.edu:2101/10.3390/fi10050043

3. Jean-Philippe, R. (2018). *Enhancing computer network defense technologies with machine learning and artificial intelligence* Retrieved from http://lasalle.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwpV09T8MwED1BWRBDQYD4KOgk5gCpk_Q8VYg0FAQMiL1yY6dMLrTw__G5ThtRqQtjFCk6xdb57vndewCie30b_ckJZUqUCZWUUqmeTknEY5W6Pq5LWSbJ69AXw-zhjfLn3lMgF_JoTFjuOkv61K2nJaPmN36qk4EL2f_8ithHiu9bg6nGNuzEXL3w-G-zIFr17-6glSmrAQYZnvo5W8vK_qgp2rCkGQTvBFfest_Jmv5tEHL8V_z7sJc3LuQPYMvYQ1AD-8EyHHaCtekDvi7o4pibyjW-BpeQvOu0kcFcfPG0TINBsXWCymq8m3kuktvk-NgQ_zyCq2Lwfj-M6pBHYU_PR6t4xTG07NSaE8C4qqSShiVnlKu8tKIk1lKXhgQlYqxPobPpS2ebX5_DritQaAF5dKD1PfsxFyzO5X_8pV_bX8hhum0

4. Jose, S., Malathi, D., Reddy, B., & Jayaseeli, D. (2018). A survey on anomaly based host intrusion detection system. *Journal of Physics: Conference Series, 1000*, 12049. doi:10.1088/1742-6596/1000/1/012049

5. Harel, Y., Gal, I., & Elovici, Y. (2017, May). Cyber Security and the Role of Intelligent Systems in Addressing its Challenges. Retrieved from http://delivery.acm.org/10.1145/3060000/3057729/a49-harel.pdf?ip=100.14.153.157&id=3057729&acc=OPEN&key=4D4702B0C3E38B35.4D4702B0C3E38B35.4D4702B0C3E38B35.6D218144511F3437&__acm__=1543206791_d4a18011d3946afb2384998007d8ea6d

6. Chordas, L. (2017). *Raising the risk level: Artificial intelligence creates new risk exposures for insurers and policyholders* A.M. Best Company, Inc. Retrieved from http://lasalle.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwtV1LS8NAEF58gIoH329lL3qRFDebx67gQdT6oCLUinoqm2SjPdhKtoI_35ltHm1F0IOXpUxCKPkmM7M7M98Qwt3akTNmE2JfiIArL5ZKhYkvOIuUD_s4VwSBFJaHvn4VXDbFeSO8qUZuVrJ_BR5kAD020v4B_PKhIIDfoAKwghLA-is1aKqOKTqimlhG3sAqIXscmNkyITu0Y5iX04aR2uCs8UHhuf587-E5omVusMXrGXb9WoYByyqMGay8kL7MD2vsJQnNWO7h7BX2uoMWskYv6wwfOYAbK4rXciWp3dYO8TmFzfpWtomzch1fDtpDa9rKXIgtHdjgPY3Y3sr4jlnS0Ks8VJGVv76rjwqtH_bBDYNh4d4BsqW_JZ24f6K7zsP9JJmG6NWa6_DxucwtMWnpl8v_mDvj-cqLthbJQsHvTU8H0C2RCd1dJjNFP8IymS1ax80K6eRoUkCTIprUonlMKyzpMJY0x5IClhSxpCWWFLCkBZYUsKQjWK6SVv2idXbl5LMynJfgyHO8AKKMlEmZ-hFEwFzDrh4Hn3osjhlPQt-NhMQSg5QzN4GoTEstlIyF0CwIopCvkalur6s3CGVpKpXUSCKkIJZOlPBYIpNYCy48

HiWbZB9fVzsfkgqLwWMk86I-jGmflmhsknV7H34r_UzF7fLK1o9XtslcpW87ZKqffehdJGMzOFhoz-L4BQ_YXdY

7. Cavelty, M. D. (2010). Cyber-security. *The Routledge Handbook of New Security Studies*, 154-162.

8. Lidestri, N. (2018). *The impact of artificial intelligence in cybersecurity* Retrieved from http://lasalle.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwpV1NT8MwDLVgXBCH8Sk-BorEuWhd2sw5oWmjbIgT4j6lTSpxaWGwA_8eO6RbxaRdOFaVKqtxnOfYfg9ADu760Z-YUKSISpqk0MYMbYoyzk1KedwAldLoeeizqXp8wcnz8Ck0F_JoTFjuJkr60G3rgm_NKW1PuAio-sn9-0fEOlJcbw2iGruwFzN64fHfNiBa5-900NJGJ38NNDyr542o7CNn1oVVm0HQTiB4y3onG_y3gcjxX_YfwsGkVZA_gh1XHUO3kXoQYeefgCJ3EjM_USnqUowWvsWIfFfMWpye4q0S4--cEGVQxTuF2-zhdTyNGtPmwXc_52u75Bl0qrpy5yDistRGO6aWMYSwrMEkttoWDiUmMrcX0Nv2pcvtr69gn4AI_l5t9KDztVi6aybh8j_4xq_hD9YnsAI

9. Qu, F., Zhang, J., Shao, Z., & Qi, S. (2017). An Intrusion Detection Model Based on Deep Belief Network. Retrieved from http://dbproxy.lasalle.edu:2334/10.1145/3180000/3171598/p97-Qu.pdf?ip=139.84.48.224&id=3171598&acc=ACTIVE%20SERVICE&key=A792924B58C015C1%2EC8B3155F0CA192F4%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&__acm__=1538442602_0cdcb0d2f23f952092ef773ca1cb7a2f

10. De Donno, M., Dragoni, N., Giaretta, A., Spognardi, A., Institutionen för naturvetenskap och teknik, & Örebro universitet. (2018). DDoS-capable IoT malwares: Comparative

analysis and mirai investigation. *Security and Communication Networks, 2018*, 1-30. doi:10.1155/2018/7178164

11. Feizollah, A., Anuar, N. B., Salleh, R., Amalina, F., & Shamshirband, S. (2013). A study of machine learning classifiers for anomaly-based mobile botnet detection. *Malaysian Journal of Computer Science, 26*(4), 251-265.
12. Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., ... & Anderson, H. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. *arXiv preprint arXiv:1802.07228*.
13. Awadi, Aymen Hasan Rashid Al, & Belaton, B. (2015). Multi-phase IRC botnet and botnet behavior detection model. doi:10.5120/11164-6289
14. Whitman, M. E., & Mattord, H. J. (2017). *Principles of information security*. Boston, MA: Cengage Learning.
15. Roosmalen, J. V., Vranken, R., & Eekelen, V. V. (2018). Applying deep learning on packet flows for botnet detection. Retrieved from http://dbproxy.lasalle.edu:2334/10.1145/3170000/3167306/p1629-van_roosmalen.pdf?ip=139.84.48.224&id=3167306&acc=ACTIVE%20SERVICE&key=A792924B58C015C1%2EC8B3155F0CA192F4%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&__acm__=1540249643_258c3c20234aa1d3286f4265ed5866c4
16. Wilner, A. S. (2018). Cybersecurity and its discontents: Artificial intelligence, the internet of things, and digital misinformation. *International Journal, 73*(2), 308-316. doi:10.1177/0020702018782496

17. Tecuci, G. (2012). Artificial intelligence. *Wiley Interdisciplinary Reviews: Computational Statistics, 4*(2), 168-180. doi:10.1002/wics.200

18. Polson, N. G., & Sokolov, V. (2017). Deep learning: A bayesian perspective. *Bayesian Analysis*, *12*(4), 1275-1304. doi:10.1214/17-BA1082

19. Fortinet. (2018, September 14). Using AI to Address Advanced Threats That Last-Generation Network Security Cannot. Retrieved from https://ready.fortinet.com/network-lead-rapidly-changing-advanced-threats/using-ai-to-address-advanced-threats-that-last-generation-network-security-cannot