AI in Cybersecurity

STS Research Paper
Presented to the Faculty of the
School of Engineering and Applied Science
University of Virginia

By

Nitesh Parajuli

05/05/2020

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Signed: _____

Approved: _____ Date _____
Rider Foley, Department of Engineering and Society

Introduction

Cyber-attacks have been increasing at an alarming rate. Human intervention is not nearly enough against mutable attacks like computer worms and viruses. According to Dilek, Cakir, and Ayudin (2015), humans cannot respond in time to form an analysis of the attack and develop an adequate response plan. The amount of information a cyber officer needs to analyze is massive, and analyzing it is one thing, but responding to an attack in time is another problem. These tasks are also tedious and repetitive. A solution to solving repetitive labor is already present. The use of computer technologies that automates manual labor. Therefore, cybersecurity also needs a stronger solution. The most promising solution is Artificial Intelligence, but it is not fully integrated within cybersecurity.

To understand why AI is even needed, a network theory is built to realize each actant and how actions of each actant lead to the conclusion that AI can solidify the cyber defense. The actor-network theory was introduced by Bruno Latour, to understand the different combination of elements or actants and interactions between them (Latour, 1992). The actants include humans like cybersecurity officers, Internet users, and hackers. It also includes non-human actants like organizations fighting cybercrimes and social media.

Enforcing Artificial Intelligence to deal with cybercrimes is based on the fact that cybersecurity officer cannot do enough to battle these crimes and the shape of the cybercrimes are drastically changing at a pace which only AI can withstand. Tedious and repetitive tasks are delegated to the cybersecurity officers, as well. To change cybersecurity measures, AI needs to be the sole delegator in solving the problem of doing those menial tasks. It leads to the question of how capable will AI be in comparison to human delegators or other measures in place to fight cyber threats. The research will address the effect of implementing AI in cybersecurity for

stakeholders like social media, cyber security officers and companies investing in artificial intelligence for cyber security.

Case Context

Artificial Intelligence focuses on applying machine intelligence to machines similar to the natural intelligence found in humans. It has had a significant impact on the real world. Facebook has implemented face recognition to identify people in a picture. Alexa can listen to the human command and interprets it with a reply. Tesla has made its Model 3 car to be a semi-auto pilot, allowing the car to come towards the car owner from a parking spot automatically. These are some of the applications achieved through applications of artificial intelligence.

Behind the scene, the resources required to power an application of artificial intelligence are massive. A significant blockade most organizations face is the scalability of their applications. Scalability is when the data for the application grows. The application must support the increase of data. Otherwise, it could face server crashes. The central aspect of artificial intelligence is data, and the way an organization collects and uses the data can make a difference. While collecting data, the application must be efficient, and to support data growth, and it must also be scalable. It also means they need more robust encryption to protect the data from being leaked. The data could be inaccurate and supports outdated models, which could alter the AI applications to behave accordingly. Processing the gathered data is also a massive task as it requires high powered GPUs for multiple large data sets. GPUs have specific processing architecture for AI applications making them powerful and efficient to use (Violino, 2018).

Cybersecurity is applied to protect the computer system and networks from theft, disruption, misdirection, and damages done to hardware and software. There has been a

considerable increase in investing in cybersecurity, as noted from Statista, that at least 66 billion U.S dollars have been spent in cybersecurity. The biggest threats and vulnerabilities are within internet application software. These threats include stealing private information of the public, stealing money from large corporations, and accessing user data from websites. The means to be a threat comes from software applications that can infect computers and extract information from them. Cybersecurity agents are not enough to deal with these computer-generated threats, which is why Artificial Intelligence needs cybersecurity.

With Artificial Intelligence integrated within cybersecurity, many of the arduous tasks like combatting machine level language programs will be much more convenient and much faster. Currently, many companies are investing in artificial intelligence to power up their infrastructure's security. Cybersecurity companies like Cylance and CrowdStrike have raised $120 and $481 million, respectively, and $500 million from funding's. The Department of Defense has also ventured to fund $1.7 billion to form Joint Artificial Intelligence to further research AI (Krause 2018). The worry for the threats does not stop at just normal programs because the level of threat also comes from Artificially Intelligent software. As noted by Krause (2018), hackers are using social media sites to mine data about the users. Hackers are malicious users who use vulnerability in a system to infiltrate and commit cybercrimes. They can use that data to create propaganda like the one seen during the 2016 election on Facebook. These are just new threats as more could follow with the progressing AI.

While Artificial intelligence seems promising in developing a new form of cybersecurity, other nations are going even further by exploiting massive groups of people through the application of AI technologies. In the 2016 election, millions of Americans were exposed to fake news and propaganda. These influences affected the choice voters would make in picking a

candidate for the 2016 election. Twitter was the primary source of fake news and strategic propaganda. The attackers were identified to be the Russians, and their attacking method had different applications of AI in creating fake news and propaganda (Horowitz et al. 2018). Horowitz and his group talk about various aspects of AI against these attacks. To counter disinformation and fake news, a new prospect is already making progress. In 2017, Google, Poynter, and MIT formed a partnership to research natural language processing and deep learning to detect misinformation. They built an algorithm to detect these nuances with an 80% success rate (The Poytner Institute, 2018).

Investing in AI as a cybersecurity detergent

The research will look at different actants that are responsible for the need of AI in cyber security. This will help to address what problem current cyber security is facing and what problems will be encountered as a result of implementing AI. It will also be a helpful tool to understand how the different actants in this network relate and affect one another. The first actant in this network is the Internet. The Internet, on its first basis, served as a communication tool and as an information provider. Now, it is the leading cause of increasing number of cybercrimes and variety in cybercrimes (Dilek, 2015). The Internet is open for hackers and malicious actors that prey on users in the Internet, to steal their information and misuse that information. The user is also part of this network, and the hackers are subparts of the users. These malicious actors are human, so they cannot understand a machine's language. They have created human-readable programs that translates to machine languages, such as malware, virus, or worms, to penetrate the users on the Internet. There are countermeasures in place against such attacks, like anti-virus software. The anti-virus software detects and analyzes infected machines and prevents the

infected program from running. However, Norton, an anti-virus provider, pointed out that Antivirus alone may not be enough. They state that the threat landscape is continuously changing, so approaches to protecting information must also change (Symanovich, 2020). These complex actants also include stakeholders like organizations who are hard hit by cybercrimes that cost them billions of dollars. And finally, as pointed out in the case context social media sites were the most recent target. Social media sites like Twitter and Facebook where users were targeted with propaganda. This research will also look into such sites to understand how the attack occurred and what has the attack enforced them to do. The next actants are cybersecurity officers, trained to detect and analyze malicious forms of attack. But there is a limit to what an officer can do against a highly sophisticated attack. As Kewlani (2018) states "cybersecurity officers have been barely successful in bringing down the time it takes to acknowledge an attack ‘after it has happened,' let alone stay ahead of the curve and predict the next breach or attack much before the attackers strike the first blow." Based on the evidence pointed above, the program of action is such that because current measures are failing the stakeholders are enforced to use AI. But, the implementation of Artificial Intelligence will be inspected in terms of a sociotechnical perspective to understand whether the new measures will be enough.

The research will explore how much will humans have to delegate their control towards AI for the betterment of cyber security. It will also look towards companies and their attention towards cyber security. This will be to gain an understanding about how they will change their current security measures and how much are they delegating their security measures towards AI. This will also be looked in terms of a cyber security officer and how much of their work is being relegated towards AI. Similar, to looking towards companies this research will also look at how

social media is adapting to AI attack measures. Especially, how much of their investment is in cyber security and how much of the security work is being delegated towards AI.

The research will look towards how this implementation of technology will affect cyber security officers. As aforementioned, their inability to stop a cyber-attack led to this decision of turning towards Artificial intelligence. This can be looked from the discrimination frame which will share insight how cyber security officers will be affected. This primarily concerns with their ability to stop cyber threats that AI will replace. The research will also look towards social media and how their inability to stop propaganda led to the massive breach of the 2016 election process. It will be to understand how the social media companies are responding to such complex attacks. In that matter, this will provide a perspective of how these measures will impact internet users that use these social medias. This will also be looked through the discrimination framework to understand whether internet users will have continuously negative impact because of AI or will new measures using AI stop the spread of misinformation.

Methods and Resources

The question that will be addressed by this research follows as such: How will the implementation of AI in cybersecurity effect stakeholders like organizations, social media and cyber security officers.

By drawing upon delegation to technologies, the program of action and discrimination the technology was assessed critically and appreciatively. These tools provided tremendous help to build criticism and appreciation for the technology. A video interview conducted by Infosec offered evidence from a cybersecurity expert about the current state of artificial intelligence in cybersecurity. The expert provided information about how AI would affect cybersecurity officers

and how AI would also help with cybersecurity. The expert is Eric Stevens, Vice President of Engineering and Principal Architect at ProectWise. Also, a case study by Kertysova et. (al) (2018) shows how implementing AI can have algorithmic bias and results in discriminating certain groups. Some sources showed an increase in investment of Artificial Intelligence. Then, there are sources that shared the profitability of investing in AI which showed a direct relation as to why companies are also invested in AI. Another source was used to look through the lens of discrimination framework which explored those affected by AI such as cyber security officers and regular workers. And lastly, some sources showed that companies were losing a lot of money because of cyber-attacks**.**

Results

It was determined through this research that while even though AI is needed towards cyber security it has flaws. AI itself has not reached its potential as it has shown high false positive, it has not reached to a level where it can function as an independent tool. It was also shown that any company will try to seek more profit and if the profit results in replacing humans with AI they will do so without hesitation. It was also shown that AI's data can be corrupted with bias such that it resonates the ideas of the polluted data. Overall, the evidence has shown that AI will have full control and will replace the current cybersecurity measures which also means they will replace cyber security analysts. While they might not be where they need to be as of now, but in the future AI will likely be the cybersecurity agent.

Cybersecurity officers

Cybersecurity officers are trained to detect and analyze malicious forms of attack. However, there is a limit to what an officer can do against a highly sophisticated attack. As Kewlani (2018) states "cybersecurity officers have been barely successful in bringing down the time it takes to acknowledge an attack ‘after it has happened,' let alone stay ahead of the curve and predict the next breach or attack much before the attackers strike the first blow." These are just a small part of the problem as Stevens (2019), states “there is more in demand for cybersecurity jobs than there are people to fill it”. These are just the basic subproblems that demand immediate attention for a fix. To fix this issue, the concentration towards Artificial Intelligence has risen drastically. Companies have delegated a non-human technology such as AI to address this issue.

Evidence shows that AI will not decentralize cybersecurity jobs. Stevens states that AI is actually being deployed to empowered humans and not completely replace them. The International Information System Security Certification Consortium “estimates that the U.S. cybersecurity workforce would need to increase by 62%” (Casesa, 2019). AI also has the problem of having false-positive rates of 50% or higher. Ponemon Institute and SIEM provider Exabeam shows that as much as a 25% of a security analyst's time is spent chasing false positives sifting through erroneous security alerts or false indicators of confidence before being able to tackle real findings. It shows that AI is just not at the level where companies want it to be. Therefore, cybersecurity jobs are more likely to be in demand for the next few years (Chickowski, 2019). This fear of AI replacing jobs also seems unfounded because AI is just not at the level of being fully operational. They can do menial tasks such as processing large amounts of data which would be inefficient for a cybersecurity officer to do.

This new paradigm, while quite revolutionary, will replace lower-level employees. If AI is implemented, they will need a new category of experts to train the AI technology. It will require organizations to either hire humans already trained to do so or have existing team members to learn even more cybersecurity-related skills. It also means that these companies are susceptible to hire analysts who can adapt to new technologies. They can discriminate against workers who are more comfortable with their current skill level and less than likely to change to new technologies (Rizkallah, 2019). Stevens stated that AI could have the potential to replace level one analyst jobs eventually, but senior-level jobs are less likely to be threatened.

Social Media

In the 2016 election, millions of Americans were exposed to fake news and propaganda. These influences affected the choice voters would make in picking a candidate for the 2016 election. To understand this attack observing the different forms of actants is also necessary. Twitter was the primary source of fake news and strategic propaganda. The attackers were Russians, and their attacking method had different applications of AI in creating fake news and propaganda (Horowitz et al. 2018). To counter this form of disinformation evidence shows that delegation to AI will address this issue.

Many pieces of evidence show that highly visited web applications are heavily investing in battling this form of disinformation. Google announced a new partnership with the International Fact-Checking Network at The Poynter Institute, and MIT's the Fake News Challenge resulted in an algorithm with an 80% success rate (Chickowski, 2019). According to Facebook, 99.5% of terrorist-related removals, 98.5% of fake accounts, 96% of adult nudity and sexual activity, and 86% of graphic violence-related removals are detected by AI tools. This

form of technology will enforce that real human beings are posting information on social sites, helping to stop the spread of disinformation (Kertysova, 2018.

The biggest problem with this technology is though it battles for disinformation, it still in its early phase. AI models are still prone to false negatives/positives, for example, identifying content and bot accounts as fake when they are not. False positives can negatively impact freedom of expression and lead to censorship of legitimate and reliable content that is machine-labelled incorrectly as disinformation as mentioned earlier and shown that current AI algorithms are likely to have a high number of false positives. These algorithms are also likely to have automated human biases and personality traits of the programmer. It is because AI relies on the person who built the program and the data that it collects. These forms of discrimination could target real users, or they could likely target specific groups and block their freedom of speech. For example, in 2016, Microsoft's Tay Bot was released in twitter to provide meaningful conversations with humans, and it would automatically talk without the assistance of humans. It would learn from the conversation with the users to have a human-like conversation. However, Twitter users populated Tay Bot's learning data with inflammatory information which caused mayhem. It would repeat after users who posted the inflammatory comments (James Vicent). These kinds of biases inserted into a data is a significant issue which would make the algorithm itself biased towards certain groups. This form of bias is noticeable as Donald (2019) pointed out that "Computer scientists shaping AI today are predominantly male, white, and well paid". Considering the lack of diversity in the computer science field, it has reflected bias of the programmer within the program. This suggests that their job is at risk, which can only be confirmed to how the research in organizations will show. As, research on cyber security officers has already suggested that their job is at risk.

Organizations

Companies are losing almost $400 billion a year, according to a British insurance company named Lloy'ds of London. (Yakowicz, 2015). These kind of loses are detrimental to these companies, and these kinds of cyber-attacks are rising even more with much more complexity. The loss of value is enormous, but the loss of personal information of stakeholders in the company puts the company in an untrustworthy place. They could lose those customers because the company is not doing enough to deal with these loses. The suffering is not just affected at the time of the attack, but it could also halt business activities after the attack. It could result in even more loses as they have to spend the time to reset the business. The problems that are the most common to notice is that current security technologies are failing miserably (Mitchell). However, because of the recent developments of Artificial Intelligence Technologies, some of the companies have delegated their security assurances to AI.

Companies like "Cylance in June completed a $120 million funding round, bringing its total to nearly $300 million. CrowdStrike has raised $481 million, including a $200 million funding round in June" (Krause 2018). The rise of investing in AI is not just in the commercial companies, in fact, "the federal government plans to spend almost $1 billion in nondefense artificial intelligence research and development in fiscal 2020, according to a supplemental report to the president's budget request" (Vincent, 2019). There is a reason for these companies and government organization to invest in AI. Its already shown that AI has the potential to change the landscape of security completely. But there is also the potential for looking towards the future where their profitability could increase. In fact, according to a report from Accenture, "businesses that successfully apply artificial intelligence (AI) could increase profitability by an average of 38% by 2035". The investment in AI "could lead to an economic boost of US$14

trillion in additional gross value added (GVA) across 16 industries in 12 economies" (Ismail, 2017). It seems that AI is enforcing businesses to move towards this route because there is a potential of huge profits in the future, and more security compared to current technologies.

Stevens mentions that a dirty little secret about companies is that they are always looking for corporate profitability (Stevens, 2019). It means that if they can find AI technologies is enough to replace humans, they will do so. This is was very evident with Amazon, as they "used a computer system to automatically track and fire hundreds of fulfillment center employees between for failing to meet productivity quotas" (Tangermann, 2019). They have delegated technology to rate a human of their productivity. These companies will discriminate their employees through the use of technology. This then confirms that programmers bias is even more likely to be risky for the companies which they can use as a leverage to fire the programmers. This means human content moderator's job is at higher risk.

Discussion

First, the actor network theory showed that because of failing cyber security measures companies are investing in AI. They delegated the jobs of security moderators to the AI technologies. Through this research its conclusive that cyber security officers will be replaced by AI technologies. However, with the current state of AI and its high rate of raising false positives AI technologies and human will have to work together for now. It was also evident that companies will discriminate against cyber security officers by replacing security jobs with an AI technology to seek higher profits. It follows like this: current security measures are failing so they delegate the security task to the non-human actor like AI. In doing so, it will negatively affect the cyber security officers, as their job is at risk. Then, there is the instance of

implementing AI for social media sites which backfired because it ended up leading to programmer's bias. And finally, evidence has shown that organizations invest in AI because of the profitability in the future with complete disregard for the workers. This research has shown that while AI will be a good detergent against the sophisticated cyber-attacks, it leads to many social problems. It negatively affects cyber security officers because they could face job loss, which was directly related to companies trying to profit. Then there is the point where the programmers bias exists which begs the question, are they even more likely to get replaced? Most of the other evidence points towards that same direction which can only mean that they will be replaced

Limitation

The most significant limiting factor of this research is that AI has not reached a level reached to a level where it can support the complex network structure. There is no way of knowing what exactly the future will look like based on how much the technology will advance. Stevens also said that we are at the point where there exists an absence of control on adversarial AI such that results can be poisoned which could cause incorrect results (Stevens, 2019). The AI technology has to reach a certain level of advancement such that extensive socio-technical research is conducted about the technology.

Future

I would have researched more about technology, similar to what Amazon has implemented. This would show more evidence to suggest that technology is driving towards controlling humans. Also, there were many details about companies and their technologies that I would have liked to explore, but they do not share such details. If this information were public, it could provide a much more understanding about the technology and its risk for employees.

Engineering Career

This makes me reconsider whether the company I am going to work for will consider me as another pawn in their game. The fear that my job will get replaced by automated technology certainly exists now. I was at the point where I considered AI to be a forefront technology, and I would later work on this technology. However, these results have made me fearful, and the biggest fear is that I could be writing a code that will get me fired.

Conclusion

This research has shown that allowing AI in cybersecurity will relegate most of the control from human to technology. In doing so, cyber security jobs are at risk and because of the boost in profits for the future, companies will more than likely invest in AI. The problem with AI does not stop there because it was evident that data collection can be polluted which allowed for algorithmic bias that the programmer reflected. It's evident that AI will discriminate against certain users because of this bias. This research has shown that AI technologies must make drastic changes to fix these issues. It is evident that AI will replace cybersecurity jobs. This research can expand to add more stakeholders like the general public. The next steps for people

is to ask whether companies are likely to change their attitude towards AI. The message is that to implement AI in cybersecurity, it must be optimized through the socio-technical lens.

References

Ahola, M. (2019). The Role of Human Error in Successful Cyber Security Breaches. *GetUsSecure*. Retrieved from https://blog.getusecure.com/post/the-role-of-human-error-in-successful-cyber-security-breaches

Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2018). On the effectiveness of machine and deep learning for cyber security. *2018 10th International Conference on Cyber Conflict (CyCon)*. doi: 10.23919/cycon.2018.8405026

Bharadwaj, R. (2019). Artificial Intelligence in Cybersecurity – Current Use-Cases and Capabilities. *Emerj*. Retrieved from https://emerj.com/ai-sector-overviews/artificial-intelligence-cybersecurity/

Browser Market Share. (2016, May). *NetApplications*. Retrieved from https://netmarketshare.com/

Cambridge, Mass. (2019). IBM Study Shows Data Breach Costs on the Rise; Financial Impact Felt for Years. (2019). *IBM Newsroom*. Retrieved from https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years

Casesa, P. (2019). The 5 Most In-Demand Cybersecurity Jobs for 2020. *Focal Point Data Risk*.Retrieved from https://blog.focal-point.com/the-5-most-in-demand-cyber-security-jobs-2020

Chickowski, E. (2019, September 02).Every Hour SOCs Run, 15 Minutes Are Wasted on False Positives. *Bitdefender*. Retrieved from https://businessinsights.bitdefender.com/every-hour-socs-run-15-minutes-are-wasted-on-false-positives

Chronicle. (n.d.). *X Development LLC*. Retrieved from https://x.company/projects/chronicle/

Donald, S. J. (2019, September 19). Don't blame the AI, it's the humans who are biased. Retrieved from https://towardsdatascience.com/dont-blame-the-ai-it-s-the-humans-who-are-biased-d01a3b876d58

Dilek, S., Çakır, H., & Aydin, M. (2015, January). Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review. *Arixv*.

Farfan, B. (2019). The New "World's Largest Bookstore" Proves That Independents Beat Chains. Retrieved from https://www.thebalancesmb.com/is-barnes-amp-noble-the-worlds-largest-bookstore-2892133.

Harris, T. R. (2018). The Comprehensive Guide To College Textbook Trends [Infographic]. Retrieved from https://www.leadwinds.com/the-comprehensive-guide-to-college-textbook-trends/.

Heinemeyer, M. (2019). Stop the clock: How Autonomous Response contains cyber-threats in seconds. Retrieved from https://www.darktrace.com/en/blog/stop-the-clock-how-autonomous-response-contains-cyber-threats-in-seconds/.

Horowitz, M. C., Allen, G. C., Saravalle, E., Cho, A., Fredrick, K., & Scharre, P. (2018). Artificial Intelligence and International Security. *CNAS*, volume(issue)1–27.

Ismail, N. (2018, May 15). AI has huge 'potential' to increase corporate profitability. *InformationAge*. Retrieved from https://www.information-age.com/ai-increase-corporate-profitability-123466950/

Kertysova, K. (2018). Artificial Intelligence and Disinformation: How AI Changes the Way Disinformation is Produced, Disseminated, and Can Be Countered. Security & Human Rights, 29, 55–81. https://doi.org/10.1163/18750230-02901005

Krause, R. (2018, November 30). AI Companies Race To Get Upper Hand In Cybersecurity - Before Hackers Do.
Retrieved from https://www.investors.com/news/technology/ai-companies-artificial-intelligence-cybersecurity/

Kewlani, R. (2018). The evolving role of AI in effectively combating cybercrime. *Fractal*.

Kingkade, T. (2017). CHART: The INSANE Growth In College Textbook Prices. Retrieved from https://www.huffpost.com/entry/college-textbook-prices-increase_n_2409153.

Latour, B. (1992). Where Are the Missing Masses? The Sociology of a Few Mundane Artifacts. In N. Name (Eds) *Shaping Technology/Building Society: Studies in Sociotechnical Change*, Cambridge, MA, MIT Press, pp. 151–180.

Quick Facts (2017). *UVA Library*. Retrieved from https://www.library.virginia.edu/about-uva-library/.

Rouse, M., & Rouse, M. (2019) What is intelligent agent? - Definition from WhatIs.com. Retrieved from https://searchenterpriseai.techtarget.com/definition/agent-intelligent-agent.

Rizkallah, J., & Rizkallah, J. (2018, October 25.). Debunking AI's Impact on the Cybersecurity Skills Gap. *Threatpost*. Retrieved from https://threatpost.com/debunking-ais-impact-on-the-cybersecurity-skills-gap/138570/

Statt, N. (2019). OpenAI's Dota 2 AI steamrolls world champion e-sports team with back-to-back victories. *The Verge*.

Stevens, E. (2019, March 6). *The Current State of Artificial Intelligence in Cybersecurity*. *YouTube (Infosec)* (2019).
Retrieved from https://www.youtube.com/watch?v=tdrE1LuPyaM

Symanovich, S. (2020). Why antivirus may not be enough. *Symantec Corporation*. Retrieved from https://us.norton.com/internetsecurity-privacy-why-antivirus-may-not-be-enough.html

Tangermann, V. (2019, April 26). Amazon used an AI to automatically fire low-productivity workers. Retrieved from https://futurism.com/amazon-ai-fire-workers

The Poynter Institute (2018). Poynter receives $3 million from Google to lead program teaching teens to tell fact from fiction online. *Poynter*. Retrieved from https://www.poynter.org/news-release/2018/poynter-receives-3-million-from-google-to-lead-program-teaching-teens-to-tell-fact-from-fiction-online/

Vincent, B. (2019, September 10). Administration Projects Agencies Will Spend $1 Billion on Artificial Intelligence Next Year.
Retrieved from https://www.nextgov.com/emerging-tech/2019/09/administration-projects-agencies-will-spend-1-billion-artificial-intelligence-next-year/159781/

Violino, B. (2018). Designing and building artificial intelligence infrastructure. *TechTarget*. Retrieved from https://searchenterpriseai.techtarget.com/feature/Designing-and-building-artificial-intelligence-infrastructure

Vincent, J. (2016, March 24). Twitter taught Microsoft's friendly AI chatbot to be a racist asshole in less than a day. *The Verge*.

Retrieved from https://www.theverge.com/2016/3/24/11297050/tay-microsoft-chatbot-racist

Yakowicz, W. (2015, September 8). Companies Lose $400 Billion to Hackers Each Year. *Inc*. Retrieved from https://www.inc.com/will-yakowicz/cyberattacks-cost-companies-400-billion-each-year.html