Artificial Intelligence, Alternative Competing Hypothesis Testing, and Fifth Generation Warfare.
Date: March 10, 2019

Disclaimer: this briefing note contains summaries of open sources and does not represent the views of the Canadian Association for Security and Intelligence Studies.

KEY EVENTS

The following key events are considered in this briefing note:

Key Event 1: The Canadian Intelligence Community met October 2018 to discuss the following themes:

1. Artificial Intelligence (AI) – Operational Context;
2. How is AI revolutionizing the Intelligence and Security Enterprise;
3. How AI will reshape the Canadian Intelligence Enterprise from a Cyber Security and Technological Perspective;
4. Technology Supporting the Intelligence Enterprise;
5. Innovation and Ethics;
6. AI and how it will transform the Intelligence Enterprise[1].

Key Event 2: Concerns were raised by Douglas Yueng, regarding the potential impact of biases in AI outputs, along with the potential vulnerability of an AI to a "bias attack" from an adversary[2] where data is manipulated or biased data inputs are intentionally supplied. Therefore, as a result of the bias that may be present, this could potentially compromise the reliability of AI outputs.

Key Event 3: In July 2017, the Royal Canadian Mounted Police announced they are "turning to artificial intelligence technology to scan millions of unknown photos and find the ones with the highest probability of being illicit — those digital needles in a haystack"[3]. Similarly, in January 2019 it was reported that "the Japanese National Police Agency (NPA) is planning to begin experimenting with the use of artificial intelligence in anti-terrorism and criminal investigations next fiscal year. The experiments would involve using the characteristics of past attacks in Europe to train AI to identify terrorists in crowded areas, and introducing AI systems to analyze surveillance videos in criminal investigations"[4].

---

[1] Canadian Military Intelligence Association, (2018.) Conference agenda for October 23rd, 2018 *ARTIFICIAL INTELLIGENCE AND THE IMPLICATIONS FOR THE CANADIAN INTELLIGENCE ENTERPRISE*, Ottawa, ON. Retrieved from https://cmia-acrm.ca/wp-content/uploads/AGENDA-19-Sep-1.pdf

[2] Yeung, D. (2018, October 22). Intentional Bias Is Another Way Artificial Intelligence Could Hurt Us. Retrieved March 8, 2019, from https://www.rand.org/blog/2018/10/intentional-bias-is-another-way-artificial-intelligence.html

[3] Aldred, K. (2017). Getting cyber smart. Gazette Magazine, 79(3). Ottawa, ON: Royal Canadian Mounted Police. Retrived from http://www.rcmp-grc.gc.ca/en/gazette/getting-cyber-smart

[4] Shepard, S. (2019, January 18). Japan is Experimenting with AI to Combat Terrorism. Retrieved from https://securitytoday.com/articles/2019/01/18/japan-is-experimenting-with-ai-to-combat-terrorism.aspx

NATURE OF DISCUSSION

These announcements suggest AI is being operationalization in a variety of national and international conflicts (war, terrorism, and crime). This briefing note will examine the implications of applying AI to 5th Gen warfare[5] and conflicts involving extremist groups and violent transnational social movements (e.g., Three Percenters (also styled III%). The scope of this briefing note is limited to examining two issues: the challenges of utilizing AI to assist with intelligence analysts decision making, and explore the potential impacts of bias found in AI outputs. After addressing these two issues, an AI model will be introduced to test in a 5th Gen warfare case study using an established structured analytical technique, i.e., analysis of competing hypotheses (ACH).

BACKGROUND

The following background information is organized as follows: Section 1 introduces AI, Section 2 explores the bias of programming and inputs which develop the AI, and Section 3 examines a hypothetical AI-driven ACH model applied to a 5th Gen incident.

Section 1 — Artificial Intelligence and the Intelligence Officer: What are the Issues?

When examining how intelligence officers can adopt AI, the following questions should be considered:

1. How do intelligence officers trust an AI product?

The AI machines used are not producing "new" information for intelligence officers, but rather will tell them information that they already know in a faster time. The recommendations that are given do not change the way the intelligence officers would come to their own conclusion.[6] However, intelligence officers caution that AI can not and should not replace the role of the human analyst. Instead, AI can help enhance the work of human intelligence analysts.[7]

Artificial narrow intelligence (ANI) — the type of AI that is currently developed — does not provide products with recommendations that have different methods of processing than what the human analysts can already do. Intelligence companies caution that AI should not and cannot replace the role of a human analyst; the AI should be there to support and enhance the human analyst's decisions.[8]

---

[5] The term '5th Gen warfare' is defined as an "identity based group-on-group conflict for the purpose of enacting a change in society." CASIS Vancouver. (2018). Retrieved from https://casisvancouver.ca/1_19_fifth-generation-warfare.html/publications/lexicon/

[6] Polonski, V. (2018, September 19). People don't trust AI – here's how we can change that. Retrieved from http://theconversation.com/people-dont-trust-ai-heres-how-we-can-change-that-87129

[7] Goldstein, P. (2017)- Why Intelligence Agencies are so interested in AI. Retrieved from https://fedtechmagazine.com/article/2017/10/why-intelligence-agencies-are-so-interested-ai

[8] Astute Solutions (n.d). Artificial Narrow Intelligence and Customer Service. Retrieved from https://www.astutesolutions.com/ani/artificial-narrow-intelligence

2. The Different Types of AI models and Their Impact on Human Trust?

There are three different types of AI. There is the aforementioned ANI, artificial general intelligence (AGI) and artificial super intelligence (ASI). As of now, ANI is the most common type of AI used; it can be found in our smartphones (e.g., Siri, Google) or home devices (e.g., Alexa, Google Home).[9]

AGI and ASI have not been developed far enough for a defined idea of their capabilities as compared to ANI; ANI is the lowest caliber of artificial technology that humans have reached.[10] However, all new ANI developments lead the pathway to AGI and eventually ASI.[11]

Furthermore, there are two types of AI models: transparent and opaque. Transparent AI is when the human can conduct analysis of the AI steps it took to reach its conclusion and justify those conclusions to a human analyst, yet it does not provide as deep insights as opaque AI would. Opaque AI comes with higher risks as the human analysts would only have a limited understanding of how the AI conducted its analysis nor generated the outputs; however, opaque AI will provide further insights than a transparent AI would.[12]

IBM says that transparency is necessary when creating AI as the human analyst needs to see the ethics and reasoning the AI used to reach its final output.[13] Pegasystems proposes something called a "T-Switch," where the 'T' stands not only for *Transparent* but also for *Trust*. If the "T-Switch" is toggled to opaque setting, than the AI will function without the ability to audit its behavior. If the "T-Switch" is toggled to transparent, then the AI must provide information about its reasoning, whilst in opaque model the reasoning is not available for analysis. Because the information is not always black and white, the "T-Switch" will be a slider ranging from 1 (very opaque) to 5 (completely transparent).[14]

3. What is the impact of AI output on Canadian decision making?

An example of the possible impact of an AI output on Canadian security decision-making can be seen in how Mastercard utilizes AI to benefit the human analyst by detecting normal and abnormal shopping spending behaviours of account holders.[15] By valuing account information like customer value segmentation, risk profiling, location, merchant, device data, time of day, and type of purchase made, it gives the AI the ability to detect and manage fraud within milliseconds. Furthermore, because it is a learning software it is able to improve its analytic abilities to an extent, to the aid and benefit the human

---

[9] Ibid.
[10] Codebots, (2018). The Three Types of AI. Retrieved from https://codebots.com/ai-powered-bots/the-3-types-of-ai-is-the-third-even-possible
[11] Sysiak, (2018). Where are we currently? - AI Revolution. Retrieved from https://medium.com/ai-revolution/where-are-we-currently-three-calibers-of-ai-8c72a9974bc
[12] Jakovljevic, P. (2017). Opaque vs. Transparent AI Explained by Pegasystems. Retrieved from https://www3.technologyevaluation.com/research/article/opaque-vs-transparent-ai-explained-by-pegasystems.html#_Toc494961813
[13] IBM, (2015). Future of Artificial Intelligence. Retrieved from https://www.ibm.com/watson/advantage-reports/future-of-artificial-intelligence/building-trust-in-ai.html
[14] Rob Walker, (2017). PegaSystems Keynote Speech.Retrieved from choosing-between-opaque-ai-and-transparent-ai
[15] Mastercard Website (n.d). Mastercard rolls out Artificial Intelligence Across its Global Network. Retrieved from https://newsroom.mastercard.com/press-releases/mastercard-rolls-out-artificial-intelligence-across-its-global-network/

analyst.[16] An AI could be utilized in a similar capacity in a national security context to assist with interpreting the implications of numerous and seemingly unrelated factors.

Section 2 — Effects of Bias on AI Development and Deployment.

AI has the potential to be fast and efficient, but is still susceptible to the bias of its human coders. The foundational level of an AI may be built in the image of its creator and includes their thoughts, views, and personality.[17] The input given to an AI to learn from is also susceptible to this bias when a human decides what data sets the AI is given.[18] For example, an AI created by the Canadian Armed Forces may very well be different from one created by ISIS or another terror organization. The AI takes on the cultures and ethical codes of conduct that are aligned with the ideals of AI's place of origin.

Two other bias need to be considered: The first, Criminal Code of Canada data sets over representation of certain ethnic populations due to past policing practices and most recently information assurance practices to improve the quality of data. The second, public health and financial records. Both, health and finance data sets, are based on legislative requirements which reflect shifting societal issues such as poverty, disease management, terrorism money laundering, etc.

The following bias can be applied to 5th Gen warfare groups and may impact the accuracy of the AI to detect based on contextual nature of operational environment. Examples of bias that may impact an AI's analysis, particularly towards 5G groups, e.g., III%er, according to IBM's "Ethics for Artificial Intelligence" [19] are as follows:

Empathy Gap: "The tendency to underestimate the influence or strength of feelings, in either one's' self or others."

The programmers may underestimate the extent of how motivated people are to follow a particular group's ideals and get involved with their activities (which then results in the AI missing the data).

Stereotyping: "Expecting a member of a group to have certain characteristics without having actual information about that individual."

The analysts' bias is not addressed — which potentially results in the AI categorizing individuals as members of an unrelated group due to a shared characteristic, i.e, miscategoring groups such as the III%er's as a one percenter biker gangs. Therefore, the AI may not adequately appreciate their membership size or the sophistication of the organization and structure under examination.

Anchoring Bias: "To rely too much on one trait or piece of information when making decisions (usually the first piece of information that we acquire on that subject."

---

[16] Pymts.com, (2018). Mastercard launches announce of AI Express. Retrieved from https://www.pymnts.com/mastercard/2018/ai-express-aml-fraud-risk-management/

[17] Osobo, O. (2018). Keeping artificial intelligence accountable to humans. TechCrunch (Aug 20, 2018). Retrieved from https://techcrunch.com/2018/08/20/keeping-artificial-intelligence-accountable-to-humans/

[18] Jones, D. (2017). AI Uninterrupted: Culture, Representation and Ethics of AI. iPass (October 13th, 2018). Retrieved from https://www.ipass.com/blog/ai-uninterrupted-culture-representation-and-the-ethics-of-ai/

[19] Cutler, A., Pribic, M., & Humphrey, L. (2018). Everyday ethics for artificial intelligence. Retrieved from https://www.ibm.com/watson/assets/duo/pdf/everydayethics.pdf 14

The could potentially result in a incorrect analysis by the AI if the initial inputs are overvalued in the assessment and not properly corrected by additional data. Furthermore, for the intelligence analysts, this may lead to the belief that AI-assisted reports are not grossly inaccurate and infallible.

Bandwagon Bias: "The tendency to do or believe things because many other people do (groupthink)."

The dominant opinion may be followed and other options may not be explored or questioned properly. An AI or AI generated product may be particularly susceptible to this form of bias.

Bias Blind Spot*:* "The tendency to see oneself as less biased than others, or to be able to identify more cognitive biases in others than in oneself."

Intelligence analysts may view an AI's findings as more objective than a humans because the analyst may not be familiar with AI constructs. It is also possible that analysts and decision-makers may be skeptical of the findings in AI-generated intelligence products and therefore ignore AI reports.

Confirmation Bias*:* "The tendency to search for, interpret, or focus on information in a way that confirms one's preconceptions."

An AI will look for what it believes to be important as determined by its developers. Therefore, an AI may search for certain features, personality types when examining groups like III%'s or its individual members, potentially leading to false positives based on the preconceived notions of the AI development team.

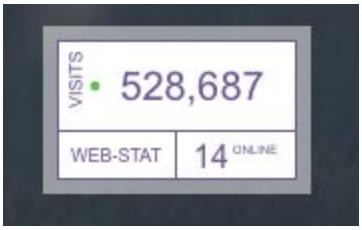
Section 3 — AI and ACH model applied to a 5th Gen event.

This section will examine how an AI may utilize ACH to conduct analysis of a 5th Gen threat. This briefing note will examine how an ACH will assist in determining the identity of a group following an incident. In this example, the group which perpetrated the incident shares similarities with the III%er's (aka 3 percenters, or, more commonly called "3pers".

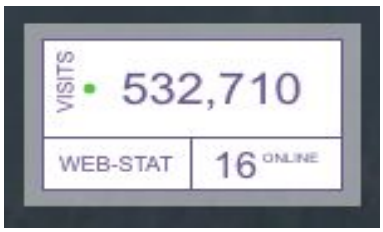
The 3pers have been described as a "anti-Muslim militia", which has allegedly targeted other groups that are viewed to act against their values and interests.[20] Therefore, in accordance with the definition of 5th Gen, the change they are trying to enact within Canadian society is a reversal of what they perceive as the unwelcomed influence of groups that are counter to their values.

Furthermore, the 3pers have an active online following (as seen below), which would suggest that the group does not exist in isolation and that others are interested in their message. This group has been gaining traction arguably without much notice by the general public.

[20] Hutter, K. (2018, May 10). Three Percenters are Canada's 'most dangerous' extremist group, say some experts | CBC News. Retrieved from https://www.cbc.ca/news/canada/three-percenters-canada-1.4647199



- Number of hits on the 3pers' website as of October, 20 2018. [21]



- Number of hits on the 3pers' website as of October 27th, 2018.[22]



- Number of hits on the 3pers' website as of March 8th, 2019.[23]

AI-driven ACH example

Hypotheses for Group Identity:	ISIS	Hells Angels	III%er's	III%er's +1
Inconsistency score	-5	-4	-3	0
Evidence:				
Target Location	Inconsistent	Consistent	Inconsistent	Consistent
Number of Victims	Inconsistent	Inconsistent	Consistent	Consistent
Crime Type 1	Inconsistent	N/A	Inconsistent	Consistent
Crime Type 2	N/A	Inconsistent	Consistent	Consistent
Weapon 1	Inconsistent	Inconsistent	Consistent	Consistent
Weapon 2	Consistent	Inconsistent	Inconsistent	Consistent
Target Ethnicity	Inconsistent	Consistent	Consistent	Consistent

Existing
New

Marco Autelitano 2019

[21] Screen capture from Three Percenters website: https://www.thethreepercenters.org/
[22] Ibid
[23] Ibid

The ACH output for a hypothetical incident shows the AI generating a new hypothesis on the basis of the available evidence. [24] An "N/A" value is assigned when the category is deemed to be undefined, or appears to be a calculation errors which requires human intelligence analysis input to resolve and assigned a value to satisfied the conditional requirement.

In the example shown above, the first hypothesis is shown to have a high inconsistency score, with the only match being that an ISIS operative once used a weapon that was used in the 3pers incident. The second notes that the incident occured in a location where the the Hells Angels are known to operate. With the ethnicity of the target matching one that the Hells Angels are believed to discriminate against. The third shows a greater consistency with the perpetrating group and the 3pers, with the area of operations, the particular crime committed and some of the weapons used being different from what has been previously observed. Therefore, the AI has generated a new hypothesis that this is a new group, similar to the III%er's yet distinct (III%er's +1). The AI can then incorporate new evidence as it becomes available in order to update the inconsistency scores and hypotheses as needed.

The AI-driven ACH is a potential application of AI to perform a structured analytic technique (SAT)[25]. The AI-driven ACH is a hypothetical AI application to assist in intelligence analysis, where an AI engine is built for conducting an ACH analysis. With an examination of the evidence for generating the inconstancy as the neural nodes for learning, along with the reference tables/databases that would allow the AI to perform an ACH, determine inconsistencies and suggest new hypotheses.

The AI performs the steps of an ACH analysis, informed through computational linguistic-driven analysis assessing the online social media statements that are presented as hypotheses and evidence respectively. This AI-driven ACH could be used for performing both tasks of hypothesis generation and evidence/ inconsistency score evaluation. This allows the AI to generate a vast range of hypothesis based on distinct possibilities; in a 5G context, this could be applied to group identification after an incident. These possibilities are thusly eliminated as the evidence is evaluated and the inconsistency scores are determined. The final set of likely hypothesis are then used in the final product, which is reviewed by an human analyst.

The AI-ACH would be initially informed by a database of possible hypothesis to be applied. Moreover, it would also be capable of generating a new hypothesis to better reflect the available evidence. The AI will be prompted to generate new suggested hypotheses, in the event that a minimum threshold for an existing minimally consistent hypothesis is not met, i.e., a group has similarities with group X, based on the evidence examined. Therefore, the AI will now consider the hypothesis that this is a new group (labeled X+1) and continue to assess this as a possible hypothesis as new evidence becomes available.

The mechanics of determining consistency works on treating consistency as a conditional statement, (E_n->H_n). Using a computational linguistic-driven analysis of both statements to determine a true/false value and the validity of the conditional statement. For the conditional to be valid, if value for E is true,

---

[24] Osoba & Welser IV, 2018, An intelligence in our image., Retrieved from www.rand.org/t/RR1744

[25] Originally designed by Heuer (1999) to assist in analysts decision making - ACH (analysis of competing hypotheses))is an analytical technique where an analyst evaluates multiple hypotheses and attempts to disprove them based on the available evidence. The hypotheses with the lowest inconsistency score is considered to be the most likely, and will be reformulated and reevaluated to reflect the available evidence. Kelshall, C., Khera, A., & Canadian Association for Security Intelligence Studies. (2018). *Introduction to structured analytical techniques for national security analysts : Tradecraft coursework and table top exercises. Volume 1 / editors, C.M Kelshall & Asha Khera.* (First ed.) Chapter 4 ACH [Manz, C. and Khera, A.], 77 - 90.

then the H must also be true. Therefore, "E" can be considered consistent with "H" for the purpose of an ACH evaluation if this conditional relationship is verified by the AI assessment of the phrases under examination.

KEY POINTS OF DISCUSSION AND WEST COAST PERSPECTIVES

Recommendation 1: Create a challenge with a monetary award to build AI capable of intelligence analysis. In 2017, the U.S. Office of the Director of National Intelligence (ODNI) launched the "Xpress" Automated Analysis Challenge, a $500,000 challenge to: "...explore AI-based opportunities for generating analytic products that surpass those crafted by traditional, highly-trained IC analysts. Leveraging private-sector momentum in this area will help ensure that the IC continues to employ cutting-edge methodologies and tools to quickly warn and inform policymakers in an ever more demanding and complex global environment."[26] Conduct research which examines the impact of the spectrum from transparent to opaque on intelligence product output

Recommendation 2: National security intelligence analysts need to be properly trained on what AI is and what it is not and understand the potential for AI to generate unreliable analysis in certain circumstances, e.g. bias in neural networks, limitations of AI, the role of the programmer, and the role AI plays in supporting decisions and not making decisions. The learning outcomes to include deeper understanding of ethics and AI, data and human bias coded into AI, and forensic analysis of AI decision making.

Recommendation 3: Broaden the scope of public engagement and education to explore various AI systems and their contributions to public safety and national security. Public consultation can guide the adoption of AI, promote AI as a valid tool for the intelligence professional to use (with the public support needed). Promote an ethics debate which is grounded in forensics, law, human rights, public policy and governances. Promote the essential role of AI as a means to augment the human decision making process in the current information society.

[26] Office of the Director of National Intelligence (2017) DS&T AND OUSD(I) LAUNCH "XPRESS" AUTOMATED ANALYSIS CHALLENGE. Retrieved from: https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2017/item/1759-ds-t-and-ousd-i-launch-xpress-automated-analysis-challenge

REFERENCES

Astute Solutions. (n.d.). Artificial Narrow Intelligence and the Customer Experience. Retrieved from https://www.astutesolutions.com/ani/artificial-narrow-intelligence

Canadian Military Intelligence Association, (2018) Conference agenda for October 23rd, 2018 *ARTIFICIAL INTELLIGENCE AND THE IMPLICATIONS FOR THE CANADIAN INTELLIGENCE ENTERPRISE*, Ottawa, ON. Retrieved from https://cmia-acrm.ca/wp-content/uploads/AGENDA-19-Sep-1.pdf

CASIS Vancouver. (2018). Retrieved from https://casisvancouver.ca/1_19_fifth-generation-warfare.html/publications/lexicon/

Codebots. (2018, July 27). 3 Types of AI: Is the Third Even Possible? Retrieved from https://codebots.com/ai-powered-bots/the-3-types-of-ai-is-the-third-even-possible

Cutler, A., Pribic, M., & Humphrey, L. (2018). Everyday ethics for artificial intelligence. Retrieved from https://www.ibm.com/watson/assets/duo/pdf/everydayethics.pdf

Goldstein, P. (2017, October 13). Why Intelligence Agencies Are So Interested in AI. Retrieved from https://fedtechmagazine.com/article/2017/10/why-intelligence-agencies-are-so-interested-ai

Hutter, K. (2018, May 10). Three Percenters are Canada's 'most dangerous' extremist group, say some experts | CBC News. Retrieved from https://www.cbc.ca/news/canada/three-percenters-canada-1.4647199

IBM. (2015, September 11). Building Trust in AI. Retrieved from https://www.ibm.com/watson/advantage-reports/future-of-artificial-intelligence/building-trust-in-ai.html

Jackson, B. (2018,May 17).IT World Canada. Holding AI accountable: Public leaders organize to ensure algorithms influencing government are ethical. Retrieved from: https://www.itworldcanada.com/article/holding-ai-accountable-public-leaders-organize-to-ensure-algorithms-influencing-government-are-ethical/404793

Jakovljevic, P. (2017, Oct 5). Opaque vs. Transparent AI Explained by Pegasystems. Retrieved from https://www3.technologyevaluation.com/research/article/opaque-vs-transparent-ai-explained-by-pegasystems.html#_Toc494961813

Jones, D. (2017).Culture, Representation and the Ethics of AI. (2017, November 02). Retrieved from https://www.ipass.com/blog/ai-uninterrupted-culture-representation-and-the-ethics-of-ai/

Kelshall, C., Khera, A., & Canadian Association for Security Intelligence Studies. (2018). *Introduction to structured analytical techniques for national security analysts : Tradecraft coursework and table top exercises. Volume 1 / editors, C.M Kelshall & Asha Khera.* (First ed.) Chapter 4 ACH [Manz, and Khera], 77 - 90.

Mastercard (n.d.). Mastercard Rolls Out Artificial Intelligence Across its Global Network Retrieved from https://newsroom.mastercard.com/press-releases/mastercard-rolls-out-artificial-intelligence-across-its-global-network/

Office of the Director of National Intelligence (2017). DS&T AND OUSD(I) LAUNCH "XPRESS" AUTOMATED ANALYSIS CHALLENGE. Retrieved from: https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2017/item/1759-ds-t-and-ousd-i-launch-xpress-automated-analysis-challenge

Osoba, O. (2018). Keeping artificial intelligence accountable to humans. TechCrunch (Aug 20, 2018). Retrieved from https://techcrunch.com/2018/08/20/keeping-artificial-intelligence-accountable-to-humans/

Osoba, O. & Welser IV, W. (2018). An intelligence in our image: The risks of bias and errors in artificial intelligence. Retrieved from www.rand.org/t/RR1744

Polonski, V. (2018, September 19). People don't trust AI – here's how we can change that. Retrieved from https://theconversation.com/people-dont-trust-ai-heres-how-we-can-change-that-87129

Pymnts. (2018, June 04). Mastercard Announces The Launch Of AI Express. Retrieved from https://www.pymnts.com/mastercard/2018/ai-express-aml-fraud-risk-management/

Shepard, S. (2019, January 18). Japan is Experimenting with AI to Combat Terrorism. Retrieved from https://securitytoday.com/articles/2019/01/18/japan-is-experimenting-with-ai-to-combat-terrorism.aspx

Sysiak, P. (2016, March 16). Where Are We Currently? – AI Revolution – Medium. Retrieved from https://medium.com/ai-revolution/where-are-we-currently-three-calibers-of-ai-8c72a9974bc

The Three Percenters - Original. (n.d.). Retrieved from https://www.thethreepercenters.org/

Walker, R.(2017, October 24). Choosing Between Opaque AI and Transparent AI. Retrieved from https://www.pega.com/insights/articles/choosing-between-opaque-ai-and-transparent-ai

Yeung, D. (2018, October 22). Intentional Bias Is Another Way Artificial Intelligence Could Hurt Us. Retrieved from https://www.rand.org/blog/2018/10/intentional-bias-is-another-way-artificial-intelligence.html