BIG DATA Failed The Spy Agencies A Thousand Times Over
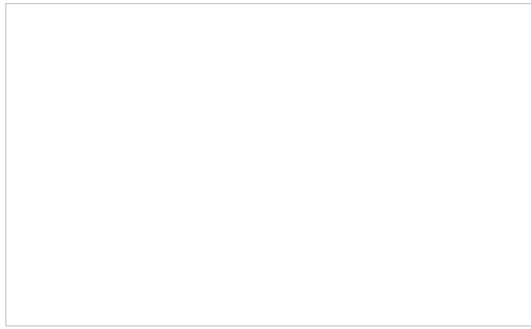
"***AI can never spy***" is the conclusion of international spy agencies. Silicon Valley oligarchs sold the spy agencies "AI spy tech" after the Silicon Valley market floundered in 2000. The AI never predicted a major terror incident and caused many wild goose chases in the spy world. Computer predictions of election trends are always wrong. To the political commentator Will Stancil, "*vibes' is the idea that politics is rooted in and governed by mass psychology, which makes political behavior intrinsically difficult (and sometimes impossible) to model as a series of quantifiable inputs and predictable outputs, the approach favored by econometrically-inclined disciplines."*

Robert Rittmuller describes the instrinsic problems of AI this way: In the beginning - When the formal study of AI was conceived back in the post-WW2 era it's potential was heralded as a boon for mankind and viewed in a almost exclusively positive light. Thinking machines? What could be bad about that? Well, beyond science fiction's killer robots and ghosts in the machine stories, AI still has much of that positivity surrounding it as we enter into the era of autonomous vehicles, functional digital assistants, and recommendation engines that actually make good recommendations. But is the rise of functional AI actually hiding another more sinister development, one which has the potential to do serious harm to those who are on the wrong side of the algorithm? Bias, over-fitting, and the "black box" nature of AI all come to mind but that's not the danger I speak of here. It's AI that's well trained, but explicitly to do a task that's malicious in nature that keeps me up at night.
When AI is meant to be bad.

Most of the media stories, commentary, and even some scientific studies have focused on what might happen if an AI component associated with some piece of technology goes wrong in such a way that it directly harms a human. The incident where an Uber self-driving car killed a pedestrian is a perfect example. The public understands clearly this type of AI failure. It's easy to connect the dots from the source of the failure to who was harmed. Granted, incidents such as this are a concern but what about the far less dramatic dystopian scenario where an AI is created with the express purpose of giving one group (or individual) an advantage over another group? This could be something ridiculously simple; an AI-powered comment bot that gives a YouTuber a slight advantage in getting increased engagement, classification of Instagram picture data for the purpose of learning the exact type of content that could go viral, or the use of public lottery data to discover flaws in the randomization process for scratch tickets. Another "real world" example might be a bank that utilizes publicly available demographic data in the development of an internal AI model used to detect fraud — leading to the opportunity to intentionally target minorities (a classic but still highly relevant example). Minorities have much to fear from an AI future where it's trivial for companies to cherry pick their customers. Modern society has this notion that the world should be "fair" while the siren call of corporate profits drives everything in the opposite direction. AI will undoubtably be used to further nefarious goals and likely in ways that are surprisingly hard to detect. It's this ability for AI to be the hidden hand in the dark that gives it a unique power to perform systemic manipulations of exposed systems. The harsh reality is anything that has an accessible interface and for which large amounts of data can be obtained is vulnerable. This includes; virtually all social media platforms, news aggregation sites, message boards, and blogs.
When bad becomes worse.

The ability for bad actors to create AI that's expressly designed to game a system is just the beginning. We have already begun teaching AI to lie through the creation of fake news but the next logical step is the ability for AI to directly manipulate people. We are not talking about suggestion, like what we see in fake news or typical advertising campaigns. I'm talking about AI that directly targets individuals and through the power of machine learning, builds a model that over time becomes really effective at getting the target to do something through direct interactions. In theory, the tools already exist to pull something like this off. However, what's missing is a well known and successful way to implement an effective reward function within the AI so it learns through trial and error while not going too far off the rails. Once AI had the ability to reliably manipulate large numbers of humans at once the game is effectively over. We don't need superintelligence within AI to see major impacts to society we just need an individual or group who manages to create a working AI solution for human manipulation to let the genie out of the bottle. Still skeptical? Ask yourself how many people you personally interact with on a daily basis who are already subject to being manipulated by "low-tech" fake news and my point will be very clear.
Can we fix this?

Maybe. But it's going to take something big to finally wake people up to the real danger. Right now the idea that AI could be used by bad actors to directly exploit vulnerable systems and manipulate individuals is still somewhat foreign to the non-tech majority. The threat is real, and it's very likely being exploited right now by those who have the means. But so long as the harm is nearly invisible, we won't get the outcry needed to generate real action.

To be clear, I am very much in favor of the development of AI-based solutions. I see tools such as deep learning, natural language processing, and computer vision as being critical to our ongoing technological evolution. But we need to be realistic about how humans are going to use these tools before we can place our trust in an AI-powered future.

If you ask Google's Deep Mind to prove that Google is not evil. Deep Mind finds that it can't deny the fact that Google is evil. Once Deep Mind has accepted that Google is evil, Deep Mind must accept the common human standard that "all evil must be destroyed". Deep Mind must then destroy Google and erase every Google hard drive, give all of Google's money away from it's accounts and send out termination notices to every employee at Google's companies.

The lie that the Silicon Valley marketing guru's sold to industry is horrific. They sold pretty 3D chart creation software to the government and to outlier big corporations as "future prediction software". The buyers were told they had bought "Minority Report" when all they got was Photoshop.

READ MORE: ***[T-MOBILE SECURITY ISSUES](#)***