Ekaterina Lyubomirova

Dr. Shelton Williams

July 3, 2020

Russia's Future in AI

Russian foreign policy has increasingly become focused on cyber security. However, Russian intelligence operatives that are notorious for spreading disinformation today borrow tactics from the Cold War's Soviet disinformation campaigns (Deeks, 2019). This paper will analyze the disinformation campaign with the largest influence, the drivers behind these campaigns from a policy perspective, the growing ability of Russia to manipulate AI developments in private US companies, and the US's deterrence strategy. Finally, this paper will suggest that the US needs a tailored deterrence strategy considering the increasing threat of cyber attacks on critical structures (Wagner, 2017). After the 2016 disinformation campaigns, how is Russia using its capabilities to advance its strategic interests? And, is Russia looking to capitalize on the development of Advanced Intelligence technologies in the US? If so, what plans does the US have to counter such a threat?

Disinformation Campaigns

Russia, and even the US, has used disinformation campaigns during the Cold War and its tactics have evolved and adapted to a new digital medium. Yet, the disinformation campaign during the 2016 elections is emblematic of its sustained approach to using social media as a method that progresses its political agenda. The 2016 media campaigns focused on divisive political issues, such as race, police brutality, and the Second Amendment. Russian actors such as the Internet Research Agency (IRA) used fake websites, Facebook, Twitter, and YouTube to proport political messages, and they manipulate the platforms' algorithms to reach a wide audience using relatively inexpensive ads (U.S. Department of Justice, 2018; Dawson & Innes, 2019). According to Facebook, the company has removed 46 pages, 91 accounts, and 2 groups for violating the platform's regulations on foreign interference and has found a striking predisposition towards false Black activism that consisted of creating fake accounts to post and manage groups, as well as posing as independent news entities in regions they targeted ("April 2020 Coordinated Inauthentic Behavior Report," 2020). This is not to say that the Kremlin

believed the validity of the cause, but instead wanted to create a cohesive, yet divisive, narrative off the back of a sensitive issue in the US. Important groups in the Facebook removal include *News Front*, a news outlet from the illegally annexed Crimea, and *South Front*, which had both its Facebook page and YouTube account taken down. These outlets perpetuated conspiracies about "Big Pharma", anti-vax messages, and news that downplayed the severity of the coronavirus. Additionally, *News Front* spreads disinformation in several languages, including Spanish, reaching a growing audience in the US and Spanish-speaking countries that already dislike the US. Furthermore, some articles and posts were and continue to be monetized. For example, a *South Front* article featured a Soundcloud ad delivered by Google. This article claimed that Vitamin C cured lives in China ("EU Cites Zero Facts about Russia's Alleged Disinformation on Coronavirus," 2020). Despite the *Reuters Institute for the Study of Journalism* finding that participants in six countries - Argentina, Germany, South Korea, Spain, the UK, and the US - consider social media platforms as less reliable about COVID-19 than health authorities, scientists, and news organization, "almost a quarter of…respondents incorrectly believe coronavirus was made in a laboratory" ("Navigating the 'Infodemic,'" 2020).

After Russia's invasion of Ukraine and annexation of Crimea in 2014, Ukraine officials banned Russian broadcasts for fear of influencing public opinion. However, that did not stop Russia from influencing in both Ukrainian citizens and the West. The *American Journal of Political Science* found that "Russian television reception has, despite its conspicuous bias, resulted in substantially and significantly higher electoral support for pro-Russian parties." This can be seen in the daily news reports broadcasted in 2010–15 on Channel One, Russia's most widely watched television station. Prior to Ukrainian protests in late 2013, Ukraine received relatively little attention, even during elections. However, during the 2014 presidential and parliamentary elections in Ukraine, Russia's most popular evening broadcast news program, *Vremia*, "dedicated 31-46% of broadcast time on weekdays and 78% of its Sunday news broadcasts to Ukraine" (Peisakhin & Rozenas, 2018). Russia also used a strategy called "reflexive control" to pacify the West towards its actions in Ukraine, rendering them on the sidelines as it watches Russia dismantle Ukraine.

These tactics were developed during the Cold War, where propaganda efforts included providing fake documents to legitimate news sources in Africa and Latin America, publishing them

through Soviet-controlled media after they gained traction, and hoping that more credible sources caught on and republished the narrative. Reflexive control as a tactic appeared nearly 30 years ago and is used today to achieve military objectives, like the occupation of Ukraine. In short, the “reflex” involves imitating the enemy’s reasoning and possible behavior that causes them to make an unfavorable decision (Snegovaya, 2015).

Russian Foreign Policy, Specifically with the US

To explore the reasons behind Russia’s current media campaigns, consider Russia’s past. The breakup of the Soviet Union left a shadow over its Russian successor. Consequently, Russia's dominance ceased with the collapse of its Red Army and retracting borders, leading many in the West and Russia’s own satellites to no longer view Russia as powerful. During this time, Russia watched as the U.S. expanded its sphere of influence and spread its own world view to reach unipolarity, casting out Russia and making all important decisions without any rebuttal. Moscow's objections were brushed aside when NATO attacked Serbia in 1999 and engulfed the former Soviet satellite states in 2002. Furthermore, domestic crime surged, civil war in Chechnya broke out, and rule at the top appeared increasingly erratic (Mankoff, 2012). This is crucial, since in order to counter the U.S.'s power and get its voice heard, the Kremlin needed to overcome social and economic shortcomings. Russia has increasingly viewed the US and its allies as actors who wish to exert “political, economic, military, and informational pressure” on Russia’s dominance, making disinformation campaigns – which are relatively cheap compared to physical military infrastructure – the best option to counter the US’s and NATO’s expansion.

Additionally, Russia prefers to engage in bilateral diplomatic discussion, making it inherently opposed to organizations like NATO. Russia relies on compliant satellite governments to prop up its sovereignty and support its quest to become a Great Power and views international order as a plate with several players who retain their own sphere of influence, refraining from interference with others’. This becomes a problem as its own sphere begins to join Westernization efforts. And, as the U.S. grapples with more problems in the digital space, it no longer has its attention to key areas of interest to Russia. By "creating chaos" in the US, Russia lessens the appeal of the West's liberal order and strengthens their loyalty (Stricklin, 2020; Trenin, 2020).

AI Development in Russia

Since 2017, Russian thinking has seen the erosion of traditional military tactics with asymmetrical warfare strategies (Bendett, 2018b). Although Russia is far behind in investment in this field compared to the US and China, there is great potential for its implementation within disinformation campaigns (Apps, 2020). If Russian actors can use machine learning to manipulate algorithms, their content can reach a wider audience. This has made Russia realize that AI tools can easily be accessed, readily deployed, and combined with "traditional" digital information warfare techniques. In fact, in 2018 Russia announced it was doubling its AI development budget and ordering the Russian Ministry of Defense (MOD), the Ministry of Education and Science of the Russian Federation (MES), and the Russian Academy of Sciences to put together a conference that united domestic and international private companies and develop a 10 point plan that highlights strategic public-private relationships and goals for research and development (Bendett, 2018a):

1. **Create an AI and Big Data Consortium** - The Russian Academy of Sciences, together with the Ministry of Education and Science of Russia (MOES), the FAEI of Russia, the Ministry of Industry and Trade of Russia and the Ministry of Defense of Russia, in collaboration with Moscow State University, should create an AI and big data consortium that combines research developments in the field and implements AI technologies into the scientific, research, and industrial community.
2. **Create an "Automated Algorithms" Fund** - The Russian Academy of Sciences, together with the MES and Science of Russia, the Ministry of Industry and Trade of Russia and the MOD of Russia, should create and file a Fund for Automated Algorithms and Projects that enhance automated systems.
3. **Create a Training System for AI Specialists** - The MES and Science of Russia together with the Russian Academy of Sciences and the MOD should create an educational platform for specialists in AI. This is an important step because although there is growth in the AI market, the state needs to support educational efforts to compete with the US and China.

4. **Create an AI Lab at the Era Technopolis** – The MOD, Moscow State University and the Informatics and Development research center should create a lab for AI advancement technologies at the Era science and technology development campus where the public and private sector can collaborate on breakthrough technology like AI, robotics, and animation. The MOD plans to move 2,000 scientists and engineers to the site by 2020. Era' success depends on whether the government learned a lesson from the failure of Skolkovo, Russia's failed Silicon Valley. During the Cold War, Russia needed a way to counter the US's growing military-industrial complex. Consequently, Russia's scientists worked in secret science cities across the country. These cities focused on specific science and technology laboratory or with an institution dealing with nuclear, biological, chemical, rocket, and ballistic technologies.
5. **Create a National Center for AI** – The Russian Academy of Sciences and the Foundation for Advanced Studies (FAS), Russia's Defense Advanced Research Projects Agency (DARPA), should create a National Center for AI which will assist in the creation of a scientific reserve, the development of an AI innovative infrastructure, and the implementation of theoretical research and promising projects in the field of artificial intelligence and IT technologies." In comparison, the US military tried something similar with the Joint AI Center (JAIC) and China's AlphaGo win. The FAS reports to the Russian President and some of its planned projects including "creating AI prototypes in image recognition, training and imitating the human thought process, complex data analysis, and assimilation of new knowledge".
6. **Monitor Changes in Global AI Development** - The MOD, along with the MOES and the Russian Academy of Sciences, should monitor changes in the AI field in other countries. The goal of this initiative is to understand the "social sciences" impact of AI.
7. **Create and Conduct Military AI Wargames** – The MOD should organize a series of military wargames, with the intention of AI models changing the nature of military operations.

8. **Check AI Compliance** – The Foundation for Advanced Research, together with the Russian Academy of Sciences, the Ministry of Education and Science of Russia and the Federal Agency of Scientific Organizations, should create proposals for a system to assess the compliance of "intellectual technologies".
9. **Discuss Proposals at the Military - Industrial Forums** – The proposals would be considered by all "interested federal executive bodies" at the "Army-2018" and the "National Security Week" forums.
10. **Hold an Annual AI Conference** – The MOD, MES, and Academy should hold an annual AI conference.

This plan highlights the government's role in this rapidly evolving field. However, absent are concrete steps to involve the private sector with the process, and the most that is said can be read between the lines. Unlike China, Russia has struggled to integrate innovations from its private sector into governmental operations, so the next best step would be for Russia to use the US's own inventions for its goals. For example, in 2016 a new set of laws called the Yarovaya amendments required telecom companies, social media platforms, and messaging apps to store data for three years and allow the Federal Security Service (FSB) access to this metadata, helping it bypass the encryption. The collection of this metadata by the FSB suggests that it is already experimenting with AI-driven analysis. One messaging platform, Telegram, refused to store and hand over this data. According to Alina Polyakova from the Brookings Institution,

> What followed was a haphazard government attempt to ban Telegram by blocking tens of millions of IP addresses, which led to massive disruptions in unrelated services, such as cloud providers, online games, and mobile banking apps. Unlike Beijing, which has effectively sought to censor and control the internet as new technologies have developed, Moscow has not been able to implement similar controls preemptively. The result is that even a relatively small company like Telegram is able to outmaneuver and embarrass the Russian state. Despite such setbacks, however, Moscow seems set to continue on a path toward "digital authoritarianism"—using its increasingly unfettered access to citizens' personal data to build better microtargeting capabilities that enhance social control, censor behavior and speech, and curtail counter-regime activities

Utilizing AI to progress its strategic influence goals would be the next step for Russia. Currently, however, Russia lacks the research and development on AI and other disruptive technologies due to its corruption and oppressive business environment. The implications of manipulating AI are still unclear, but combined with the ongoing cyber attacks, disinformation campaigns, and political influence strategies malicious actors already use, AI tools could "hyperpower Russia's use of disinformation" (Polyakova, 2019). Considering its cost effectiveness, AI would be an appealing choice for a nation who cannot militarily compare to the US.

AI Development in the USA poses ignored risk

An important thing to note is that AI can revolutionize Russia's use of disinformation, and unlike the conventional military space, the US and Europe cannot dominate. The development of machine learning capabilities will continuously learn how to improve algorithms, meaning that it will be harder to differentiate between real and fake. Russia could harness this power to manipulate information further. For example, because the influential disinformation campaign uncovered in 2017 cost about $4 million for the IRA, Russia will likely look to expand its capabilities there (Kelly et al., 2018). The accounts used in this operation took advantage of Facebook's algorithms, which favored sensitive comment at as it drove up reaction. Facebook's reaction to this was to label ad posters and other ads these accounts have posted. To reach 125 million Americans, the IRA relied on the same methods companies use to promote their products, and with the rise in audio and video manipulation techniques known as "deep fakes," it is easier than ever to produce synthetic content efficiently and cheaply. In the past, Russian disinformation has been static (news stories, ads, memes), but advances in AI – particularly from the US – will create dynamic content (video, audio). Progress in voice interaction, "deep fakes," and natural language processing has allowed AI to connect with people in a deeper way. As AI improves, it will gain more personal data and use it to personalize messages towards targeted users (Polyakova, 2019). Liesl Yearsley for the MIT Technology Review stated that "humans are far more willing than most people realize to form a relationship with AI software" (Yearsley, 2020). This is in part because people want to believe that advanced AI (with almost undistinguishable human characterizes) cares about people. AI and machine learning exploits human behavior. The products users see as ads and targeted messages are the workings of an

underlying billion-dollar industry which encompasses data collection, advertising platforms, and search engine optimization, to analyze user preference, values, and behavior.

US Deterrence Strategy

During the Cold War, the Raegan administration created the Active Measures Working Group (AMWG). The goal of this organization was to monitor Soviet propaganda, report on it daily, collaborate with Western media, and even confront Soviet officials. The AMWG was able to effectively counter Soviet propaganda efforts by undermining their effectiveness. The reason for AMWG's success was its transparency with non-governmental initiatives to counter Soviet propaganda. However, it would be harder to control the flow of information today since during the Cold War, journalists weeded out fake stories, whereas today, social media platforms typically uncover the damage and perpetrators after the attacks(s) (Deeks, 2019).

In the present, we see a more general approach towards disinformation in general. As the Internet becomes the battleground, the US faces public scrutiny, legislative pushback, and calls for a more private Internet when it handles interference. One key document that addresses cyber deterrence is Executive Order 13636—Improving Critical Infrastructure Cybersecurity. Passed by former President Barak Obama in February 2013, this order circumvented Republican refusal to create a law that required companies to share live threat information on their networks. It allowed the Commerce Department and the National Institute of Standards and Technology to come up with a framework for security standards and ways to counter interreference. Additionally, a later presidential directive known as PDD-20 authorized the Defense Department to expand its threat intelligence program beyond the defense industrial base and to "critical infrastructures." PDD-20 defined how the military would go to cyber war and that either the President or the Secretary of State could issue the order to strike. More importantly, PDD-20 instructed the military to list targets of "national importance" to the U.S. These include financial networks, electrical grids, and communication systems internationally. This was the U.S.'s first plan on case of a cyber attack. Along with the Cyber Command, the military had three principal cyber war missions, which includes "cyber protection forces" that operate and defend the US military's computer networks globally. These forces used filters to survey every piece of information that moves through the Internet, looking for indicators of an intrusion (such as worms, viruses, and traffic from suspected Internet addresses). The second mission is comprised

of teams that collect intelligence for different defense and offense departments. The third mission protects US critical infrastructure. This force only conducts offensive operations on foreign hackers trying to disable an electrical power plant or an energy grid. These forces reroute malicious traffic away from their target and report to the US Cyber Command. There is also a cyber war cabinet – which consist of an emergence conference call-system that links the law enforcement, the President, and the National Security Council. Nevertheless, 90% of the cyber force works on defense by patching vulnerabilities, guarding networks, and upgrading hardware and software. The reasons why defense is more prominent is because it is much harder to use offensive techniques as a defended and because the US has only recently made cyber warfare a priority. In a recent move, the government has encouraged companies to develop traps, or honeypots, that lure hackers into a sandbox network and infect them with malware or spyware (Harris, 2014).

Yet, none of these initiatives address interference that does not involve breaking into networks. In that case, it relies on the private sector to regulate its own content, like the American journalists did during the Cold War. However, the increasing amount of traffic on social media and the Internet has made it difficult to regulate content. The US will need to collaborate with the private sphere and develop a strategy that safeguards the companies' AI expansions and protects users from divisive content perpetuated by foreign actors.

In 2015, the US Department of Defense created the Defense Innovation Unit (DIU) to fund research surrounding the development of technologies with a defense purpose and the US established an AI Caucus co-chaired by Congressman John Delaney and Congressman Pete Olsen. Part of its plans include passing legislation addressing the US's strategy on AI (Polyakova, 2019). If the US does not develop a cohesive plan to keep its technologies from being manipulated, it faces the risk of more influential disinformation campaigns that cause further damage to an already discontent society.

Trump Administration's Approach to Russian Foreign Policy

Trump's presidency is plagued with the 2016 Russian scandal, yet his administration has been hesitant to address the issue head-on. For example, even though US security officials have consistently warned about crippling cyber attacks and adversary influence through social media, the first time the US accused Russia of hacking into American energy grids was in March of

2018 (Volz & Gardner, 2018). However, despite three separate occasions where Democratic leaders asked the Trump administration for a threat assessment on Russian cyber capabilities, the administration's most explicit move was to remove a Russian cyber security firm from its approved government list. The Kaspersky Lab, which US officials say has ties to Russian intelligence, and its removal marks "the most significant and far-reaching response yet" by the Trump administration in response to worries that Russian intelligence services with ties to the firm could exploit its anti-virus software to "steal and manipulate users' files, read private emails or attack critical infrastructure in the United States" (Levine, 2017).

In the context of Executive Order 13636, President Trump signed a complimentary order titled "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," which requires agency heads to follow the National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity. This framework was produced through Executive Order 13636 and includes a risk management model for cyber security. Additionally, Trump's Executive Order gave agency heads 90 days to produce a detailed action plan that included "risk mitigation and acceptance choices made by each agency head" (Murillo, 2019).

Overall, it is up to negotiations with Russia that will determine how its cyber force and disinformation campaigns will be tracked and monitored. Recently, Russia held a referendum that extended Putin's place in power until 2036. In fact, the Associated Press stated that that Putin was "guaranteed to get the result he wants following a massive state propaganda campaign" (Isachenkov & litvinova). Meanwhile, the US and its European allies need to address the growing risk of developing AI tools that could impact algorithms, and how to best protect the general public by cooperating with private enterprise in the face of Putin's continued rule.

Works Cited

"Building the Cyber Army." *@War: the Rise of the Military-Internet Complex*, by Shane Harris, Mariner Books, Houghton Mifflin Harcourt, 2015, pp. 39–69.

"Navigating the 'Infodemic': How People in Six Countries Access and Rate News and Information about Coronavirus." *Reuters Institute for the Study of Journalism*, reutersinstitute.politics.ox.ac.uk/infodemic-how-people-six-countries-access-and-rate-news-and-information-about-coronavirus.

Apps, Peter. "Commentary: Are China, Russia Winning the AI Arms Race?" *Reuters*, Thomson Reuters, 15 Jan. 2019, www.reuters.com/article/us-apps-ai-commentary-idUSKCN1P91NM.

April 2020 Coordinated Inauthentic Behavior Report. Facebook.

Bendett, Samuel. "Here's How the Russian Military Is Organizing to Develop AI." *Defense One*, 20 July 2018a, www.defenseone.com/ideas/2018/07/russian-militarys-ai-development-roadmap/149900/.

Bendett, Samuel. "In AI, Russia Is Hustling to Catch Up." *Defense One*, 4 Apr. 2018b, www.defenseone.com/ideas/2018/04/russia-races-forward-ai-development/147178/.

Dawson, Andrew, and Martin Innes. "How Russia's Internet Research Agency Built Its Disinformation Campaign." *The Political Quarterly*, vol. 90, no. 2, 2019, pp. 245–256., doi:10.1111/1467-923x.12690.

Deeks, Ashley, et al. "Addressing Russian Influence: What Can We Learn From U.S. Cold War Counter-Propaganda Efforts?" *Lawfare*, 31 Oct. 2019, www.lawfareblog.com/addressing-russian-influence-what-can-we-learn-us-cold-war-counter-propaganda-efforts.

Eu. "EU Cites Zero Facts about Russia's Alleged Disinformation on Coronavirus." *EU vs DISINFORMATION*, 4 May 2020, euvsdisinfo.eu/report/eu-cites-zero-facts-about-russias-alleged-disinformation-on-coronavirus/.

Gunitsky, Seva. "Democracies Can't Blame Putin for Their Disinformation Problem." *Foreign Policy*, 21 Apr. 2020, foreignpolicy.com/2020/04/21/democracies-disinformation-russia-china-homegrown/.

Hjorth , Frederik, and Rebecca Adler-Nissen. "Ideological Asymmetry in the Reach of Pro-Russian Digital Disinformation to United States Audiences Ideological Asymmetry in the Reach of Pro-Russian Digital Disinformation to United States Audiences." *Journal of Communication*, vol. 69, no. 2, 21 Mar. 2019.

Isachenkov, Vladimir. "Russian Voters Agree to Let Putin Seek 2 More Terms." *AP NEWS*, Associated Press, 1 July 2020, apnews.com/c9719e4bd8a398b8e81e49ed5304965e?utm_source=dailybrief.

Kelly, Erin, et al. "Thousands of Facebook Ads Bought by Russians to Fool U.S. Voters Released by Congress." *USA Today*, Gannett Satellite Information Network, 10 May 2018, www.usatoday.com/story/tech/2018/05/10/thousands-russian-bought-facebook-social-media-ads-released-congress/849959001/.

Legucka, Agnieszka. "Russia's Long-Term Campaign of Disinformation in Europe." *Carnegie Europe*, 19 Mar. 2020, carnegieeurope.eu/strategiceurope/81322.

Levine, Mike. “Trump Administration Pulls Russian Cyber Firm from Government-Approved List.” *ABC News*, ABC News Network, 2017, abcnews.go.com/US/trump-administration-pulls-russian-cyber-firm-government-approved/story?id=48578556.

Mankoff, Jeffrey. *Russian Foreign Policy: the Return of Great Power Politics*. Rowman & Littlefield Publishers, 2012.

Murillo, Helen. *A Summary of the Cybersecurity Executive Order*. 31 Oct. 2019, www.lawfareblog.com/summary-cybersecurity-executive-order.

Peisakhin, Leonid, and Arturas Rozenas. “Electoral Effects of Biased Media: Russian Television in Ukraine.” *American Journal of Political Science*, vol. 62, no. 3, 2018, pp. 535–550., doi:10.1111/ajps.12355.

Polyakova, Alina. “Weapons of the Weak: Russia and AI-Driven Asymmetric Warfare.” *Brookings*, Brookings, 25 Oct. 2019, www.brookings.edu/research/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare/.

Russian National Security Strategy. 2015, www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf.

Snegovaya, Maria. “Putin's Information Warfare In Ukraine: Soviet Origins of Russia's Hybrid Warfare.” *Institute for the Study of War*, Sept. 2015, www.understandingwar.org/report/putins-information-warfare-ukraine-soviet-origins-russias-hybrid-warfare.

Stricklin, Kasey. “Why Does Russia Use Disinformation?” *Lawfare*, 1 Apr. 2020, www.lawfareblog.com/why-does-russia-use-disinformation.

Stubbs, Jack. “Russia to Ban Telegram Messenger over Encryption Dispute.” *Reuters*, Thomson Reuters, 13 Apr. 2018, www.reuters.com/article/us-russia-telegram-block/russia-to-ban-telegram-messenger-over-encryption-dispute-idUSKBN1HK10B.

Trenin, Dmitry. "What Does Russia Want From the United States?" *The Moscow Times*, The Moscow Times, 3 June 2020, www.themoscowtimes.com/2020/04/17/what-does-russia-want-from-the-united-states-a70011.

U.S. Department of Justice. *United States v. INTERNET RESEARCH AGENCY LLC*. 25 June 2018.

Volz, Dustin. *In a First, U.S. Blames Russia for Cyber Attacks on Energy Grid*. 16 Mar. 2018, www.reuters.com/article/us-usa-russia-sanctions-energygrid-idUSKCN1GR2G3.

Wagner, Daniel. "The Growing Threat of Cyber-Attacks on Critical Infrastructure." *HuffPost*, HuffPost, 25 May 2017, www.huffpost.com/entry/the-growing-threat-of-cyb_b_10114374.

Yearsley, Liesl. "We Need to Talk About the Power of AI to Manipulate Humans." *MIT Technology Review*, MIT Technology Review, 2 Apr. 2020, www.technologyreview.com/2017/06/05/105817/we-need-to-talk-about-the-power-of-ai-to-manipulate-humans/.